PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-228060
(43)Date of publication of application : 15.08.2000

(51)Int.Cl. G11B 20/10
G06F 12/14
G09C 1/00
H04L 9/10
H04N 5/91
H04N 5/92

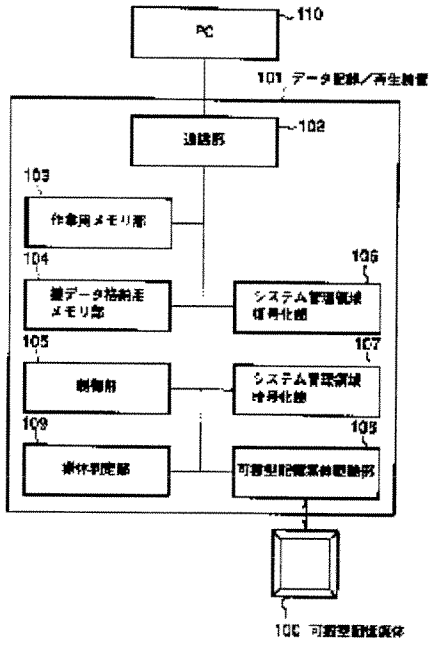
(21)Application number : 11-144928
(22)Date of filing : 25.05.1999

(71)Applicant : OLYMPUS OPTICAL CO LTD
(72)Inventor : KONDO TAKASHI

(30)Priority
Priority number : 10343013 Priority date : 02.12.1998 Priority country : JP

(54) DATA RECORDING/REPRODUCING DEVICE USING PORTABLE STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To secure the securecy and the genuineness of data by holding encryption secret information including an encryption key signal or an encryption key generating information for generating an encryption key signal and performing the cryptographic processing of data for system management while using the encryption secret information and recording the ciphered data for system management in the system management area of a storage medium.
SOLUTION: When the data received from an external PC 110 via a communication part 102 are written on a portable storage medium 100, data for system management are read out in a memory part for work 103. The data received from the external PC 110 are written on the medium 103 by using decoded data for system management. Since the constitution of the data on the medium 100 is updated, the data for system management on the memory for work 103 are also updated. The data for system management on the memory for work 103 are ciphered by using a ciphering part 107 and the ciphered data for system management are written in the system management area of the medium 100 by using a portable storage medium driving part 108.



* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]A data recorder which records data on a portability type storage which has a user area where a system management area and data for users in which data for system managements is recorded are recorded, comprising:
Encryption confidential information holding mechanism holding encryption confidential information including enciphering key signal creation information for generating an enciphering key signal or an enciphering key signal.
By encoding means which performs encryption processing using said encryption confidential information currently held at said encryption confidential information holding mechanism, and said encoding means. A recording device which carries out encryption processing of at least some data for system managements which should be recorded on a system management area of said portability type storage, and is recorded on a system management area of said portability type storage.

[Claim 2]While performing processing which data for users writes in a user area of said portability type storage, said encoding means, The data recorder according to claim 1 performing in time said encryption processing of at least some data for system managements which should be recorded on a system management area of said portability type storage in parallel.
[Claim 3]A data reproduction apparatus which reads data from a portability type storage which has a user area where a system management area and data for users in which data for system managements is recorded are recorded, comprising:
Decryption confidential information holding mechanism holding decryption confidential information including decryption key signal creation information for generating a decryption key signal or a decryption key signal.
By decoding means which performs decoding processing using said decryption confidential information currently held at said decryption confidential information holding mechanism, and said decoding means. Said said data for system managements currently enciphered and recorded is read from a system management area of said portability type storage with which at least some data for system managements uses said encryption confidential information for a system management area of said portability type storage, it enciphers to it, and is recorded on it, A data reproduction means for system managements which decodes said at least some of data for system managements currently enciphered and recorded using said decoding means.

[Claim 4]The data recorder comprising according to claim 1:
A data dividing means which divides this data for users into size of an accessible unit field logically on a portability type recording medium when said recording device records data for users on said portability type recording medium.
A record section selecting means which chooses intact unit recording areas from a user area of said portability type recording medium, A recording control means which controls record of divided data so that data divided by said division means is recorded by irregular arrangement to each field where it adjoins of two or more intact unit recording areas where said record section

selecting means was selected.

[Claim 5]The data recorder according to claim 1, wherein said recording device has a defect region registration means to register with said data for system managements by making at least one unit field into a defect region among two or more unit recording areas of said portability type recording medium in the case of processing which initializes said portability type recording medium.
[Claim 6]The data recorder comprising according to claim 1:
A random data generation means which generates random data using a parameter with which said recording device is optional.
A random data writing means which writes random data obtained by said random data generation means in the whole user area of said portability type recording medium when initializing said portability type recording medium, A parameter recording device which records said parameter on a system management area of said portability type recording medium.

[Claim 7]The data recorder according to claim 6 when said random data writing means deletes data from said portability type recording medium, wherein it is what writes said random data in a data deletion field of said portability type recording medium again.
[Claim 8]The data recorder comprising according to claim 1:
A random data generation means which generates random data using a parameter with which said recording device is optional.
A free-space selecting means which makes multiple selection of the intact field from a user area of said portability type recording medium, and a random data writing means which writes said random data in a field obtained by said free-space selecting means.

[Claim 9]The data recorder comprising according to claim 1:
unit recording areas where said recording device continues said data for users in said user area -- therefore -- it is what is recorded continuously -- unit-recording-areas ID at the tail end in inside of said continuous unit recording areas, and a head.
ID recording device which records defect region ID in said unit recording areas on a table for file management of said system management area, An address means to ask for a physical address of said data for users recorded on said portability type recording medium based on ID recorded on said table for file management.

[Claim 10]The data recorder comprising according to claim 9:
A processing means by which said data for users receives in part at least, and said recording device performs predetermined processing.
Information relevant to an address on data of a field where predetermined processing was performed by said processing means, and this address, and a processing information storage means to record at least one of parameters required for said predetermined processing on said data for system managements.

[Claim 11]The data recorder according to claim 10, wherein said processing means shuffles by a data unit in each unit recording areas.
[Claim 12]The data recorder according to claim 10, wherein said processing means shuffles in each unit-recording-areas unit.
[Claim 13]The data recorder according to claim 10, wherein said processing means performs a shuffle of to said whole data for users.
[Claim 14]The data recorder according to claim 10, wherein said processing means performs processing which enciphers data.
[Claim 15]The data recorder according to claim 10 performing said processing means combining at least two processings from inside of a shuffle in a unit field, an unit-recording-areas unit shuffle, a shuffle of to said whole data for users, and processing of data encryption.
[Claim 16]The data recorder according to claim 1 having a code extraction recording device

which records a predetermined code produced by extracting said recording device from data for users recorded on said portability type recording medium on said system management area.
[Claim 17]The data reproduction apparatus comprising according to claim 3:
A code extraction means to extract a predetermined code from said data for users which read said data reproduction means for users from said portability type recording medium.
It is said code collation means to compare, about a code extracted by this code extraction means, and said code which are extracted when recording said data for users on said portability type recording medium, and is beforehand recorded on said system management area.

[Claim 18]The data reproduction apparatus comprising according to claim 3:
A parameter reading means to which said data reproduction means for users reads said parameter from said system management area.
A means to compare random data generated using a parameter read from said system management area, and random data indicated to a cluster of a free space of said portability type recording medium.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention enciphers and records data on portability type storages, such as a magneto-optical disc (MO), and, for example. When enciphering the data recording / playback equipment, and data which reproduce the data enciphered and recorded and recording on a portability type storage, it is beforehand related with record / the data recording/playback equipment which was made to reproduce with the measure against defense to the unjust attack to a portability type storage.
[0002]
[Description of the Prior Art]As everyone knows, the art for securing the privacy of the contents and bona fides (not altered) is partly proposed from the former to contents, such as a digital image.
[0003]For example, to JP,7-122960,B. The technique of securing the privacy and bona fides of an image content is indicated by forming a random number generation device in a digital camera, and enciphering image data to the picture photoed with the digital camera using said random number system within a digital camera.
[0004]The technique of the ability to detect whether image data is altered is indicated by JP,9-200730,A by creating the electronic signature of image data within a camera.
[0005]the IS&C (Image Save & Carry) system (the department of ****** "electronic storage and IS&C system of a picture".) which is an electronic preservation system of the medical picture using a magneto-optical disc In new medical July, 1994 item P36-40. The file system and device driver of a magneto-optical disc are specialized, and the privacy of contents, such as a digital image, and bona fides are secured by preventing from accessing except software (change of data is impossible) for exclusive use.
[0006]
[Problem(s) to be Solved by the Invention]However, in the technique by former JP,7-122960,B and JP,9-200730,A, although it is possible to protect contents from the threat of disclosure of an image content, Using a general-purpose computer etc., a graphics file is accessed, a graphics file cannot be eliminated or a malicious user cannot protect contents from the alteration of the threat which destroys a data content, i.e., the image content in a large meaning.
[0007]The picture photoed with a digital camera is a size exceeding 1 million surface elements, the operation amount which enciphers the image data of such big size, or asks for an electronic signature from image data will become very large, and processing time will also become long.
[0008]Since so big a thing cannot expect the throughput of internal CPU if it tries to process a code etc. inside a digital camera especially, processing time will become so long that it cannot ignore.
[0009]This problem becomes remarkable when equipping a digital camera with a continuous-shooting function.
[0010]Like a digital camcorder device, since data size becomes large further when it comes to the data of an animation, the problem of processing time becomes still more serious.
[0011]On the other hand, in a file system for exclusive use like the latter IS&C system, since

processing of data encryption is not needed, processing time does not become a problem.
[0012]However, if it is a user who has the knowledge of a preservation apparatus etc. to some extent when the structure of a file system has been revealed, the file on a portability type storage will be able to be accessed.
[0013]When the information for protecting the safety of the file on a portability type storage is revealed like [at the time of using the technique of encryption], it cannot perform ending, if only the key to encryption is exchanged.
[0014]As a device for safety reservation of a data content, also after exhibiting the mechanism for safety reservation rather, it is desirable for safety to be securable.
[0015]An object of this invention is to provide the data recording/playback equipment which can prevent the alteration which secured the privacy of a data content, and bona fides, and includes unjust elimination and destruction of data when it stores the mass data of a picture etc. in a portability type storage paying attention to these points, and can realize high-speed processing.
[0016]
[Means for Solving the Problem]According to this invention, it is (1) in order to solve an aforementioned problem. In a data recorder which records data on a portability type storage which has a user area where a system management area and data for users in which data for system managements is recorded are recorded, Encryption confidential information holding mechanism holding encryption confidential information including enciphering key signal creation information for generating an enciphering key signal or an enciphering key signal, By encoding means which performs encryption processing using said encryption confidential information currently held at said encryption confidential information holding mechanism, and said encoding means. A data recorder having a recording device which carries out encryption processing of at least some data for system managements which should be recorded on a system management area of said portability type storage, and is recorded on a system management area of said portability type storage is provided.
[0017]According to this invention, it is (2) in order to solve an aforementioned problem. Said said encoding means, While performing processing which data for users writes in a user area of said portability type storage, time -- being parallel -- said -- portability -- type -- a storage -- a system management area -- it should record -- a system management -- ** -- data -- at least -- a part -- said -- encryption -- processing -- carrying out -- things -- the feature -- carrying out -- (-- one --) -- a statement -- a data recorder -- providing -- having .
[0018]According to this invention, it is (3) in order to solve an aforementioned problem. In a data reproduction apparatus which reads data from a portability type storage which has a user area where a system management area and data for users in which data for system managements is recorded are recorded, Decryption confidential information holding mechanism holding decryption confidential information including decryption key signal creation information for generating a decryption key signal or a decryption key signal, By decoding means which performs decoding processing using said decryption confidential information currently held at said decryption confidential information holding mechanism, and said decoding means. Said said data for system managements currently enciphered and recorded is read from a system management area of said portability type storage with which at least some data for system managements uses said encryption confidential information for a system management area of said portability type storage, it enciphers to it, and is recorded on it, A data reproduction apparatus having a reproduction means for system managements which decodes said at least some of data for system managements currently enciphered and recorded using said decoding means is provided.
[0019](Operation effect) In the above (1) or an invention of (3). An enciphering key or a decryption key (when using a cryptographic algorithm of a secret key method) for performing encryption or decryption in a data recorder beforehand A decryption key is the same as an enciphering key, or confidential information for generating an enciphering key and a decryption key is stored, When recording data on a portability type storage, Data in which information which matches a physical address and a logical address on entry data of a root directory table currently recorded on a system management area on a portability type storage or a portability type storage was stored is enciphered and recorded with said enciphering key.

[0020]Even if it is going to access said portability type storage with general-purpose data recording/playback equipment by doing in this way, since information for accessing a data file cannot be read, data cannot be accessed with a general-purpose device.
[0021]A user uses a command [low / SCSI / (Small Computer System Interface)] deeply [knowledge over a data storage device], Since it is very difficult to decode information for accessing unless a key to encryption is known, even if it reads information for accessing the above-mentioned data file, it cannot perform accessing data in practice.
[0022]Though what is enciphered is data currently recorded on a system management area of a portability type storage, for example, the whole data of a region for system managements is enciphered in a technique by this invention, There will be little processing time for size of this data to calculate encryption since it is far small compared with image data or dynamic image data, and it will end.
[0023]For example, if saved at a file, without compressing 1,300,000-pixel image data, it will become the data size of about 4 megabytes, but data size of a system management area is at most hundreds of K bytes even 1 G byte of disk in one side.
[0024]That is, when it is going to encipher image data compared with enciphering data of a system management area, in the above-mentioned example, one hundreds times the operation amount of this will be needed.
[0025]This difference will become still more remarkable if data size becomes a video data which can be hundreds of megabytes - several gigabytes.
[0026]In an invention of the above (2), stress by processing time of encryption is canceled by performing data encryption processing for system managements in parallel to time which is writing in data of an face image etc. into a portability type storage.
[0027]Usually, it differs from a processor (for example, CPU) for a processor for exclusive use being used for processing which writes data in a portability type storage, therefore processing encryption.
[0028]Even if it performs in parallel processing which enciphers writing to portability type storages, such as image data, and data of a system management area, a problem like data does not arise.
[0029]Data of a picture or video amounts to several megabytes - hundreds of megabytes, and needs time for data writing to some extent.
[0030]Therefore, it becomes possible to lose stress of processing time by encryption by performing in parallel processing which enciphers data of a system management area at the time of data writing.
[0031]A 1st embodiment that mentions the above (1) thru/or an invention of (3) later corresponds, and related figures are drawing 1 thru/or drawing 10.
[0032]According to this invention, it is (4) in order to solve an aforementioned problem. Said recording device, A data dividing means which divides this data for users into size of an accessible unit field logically on a portability type recording medium when recording data for users on said portability type recording medium, A record section selecting means which it is intact from a user area of said portability type recording medium, and also chooses a record section, So that data divided by said division means may be recorded by irregular arrangement to each field where it adjoins of two or more intact unit recording areas where said record section selecting means was selected, A data recorder given in (1) having a recording control means which controls record of divided data is provided.
[0033]A 2nd embodiment that mentions this invention of (4) later corresponds, and related figures are drawing 12 and drawing 15 thru/or drawing 17.
[0034]And it corresponds to a cluster region called accessible unit field with a FAT filesystem etc. logically under this invention of (4).
[0035]When data is recorded, drawing 15 disassembles data shown in ID=3 and a field corresponding to 12, 14, and 19 by which hatching was carried out in size of a cluster, and shows a key map which records it on a not continuous cluster.
[0036]Therefore, data shown in ID=2 and a white field corresponding to 4, 13, and 18 in this case shall not be disassembled in size of a cluster.

[0037](Operation effect) In the usual file system, when recording data, it records on a field which continued mostly physically in a user area.
[0038]Therefore, there is a possibility that the contents of data currently recorded may be unjustly read in analyzing a bit pattern which carries out direct access to a user area, and is recorded on a user area, only by the above (1) thru/or invention of (3).
[0039]On the other hand, in this invention of (4), in recording data, first, data is divided into plurality and it records that each divided data becomes discontinuous physically after that on a user area.
[0040]Therefore, even if it reads a bit pattern currently recorded on a user area by carrying out direct access, it is difficult to restore the original data from there.
[0041]As an example, a case where 6 megabytes (equivalent to image data incompressible 2 million pixels) of data is recorded on a with the total capacity of 1 G byte and a cluster size of 16 K bytes disk is considered as a portability type recording medium.
[0042]In this case, the number C of combination of sorting of possible data is C= 65200 even when data size is known, since a cluster total of an entire disk is 62500 pieces and a cluster number which constitutes 6 megabytes of file is 375 pieces! /(65200-375)!
Since it comes out, it exists also as about 65200^{375} and C cannot decode the original data in practice in round robin.
[0043]According to this invention, it is (5) in order to solve an aforementioned problem. Said recording device, said -- portability -- type -- a recording medium -- initializing -- processing -- the time -- said -- portability -- type -- a recording medium -- plurality -- unit recording areas -- inside -- at least -- one -- a ** -- a unit -- a field -- a defect region -- carrying out -- said -- a system management -- ** -- data -- registering -- a defect region -- registration -- a means -- having -- things -- the feature -- carrying out -- (-- one --) -- a statement -- a data recorder -- providing -- having .
[0044]A 2nd embodiment that mentions this invention of (5) later corresponds, and related figures are drawing 18 and drawing 19.
[0045](Operation effect) According to this invention of (5), two or more defect regions which cannot record data in a user area are arranged (in the case of a FAT filesystem). By what a code which shows that it is a defective cluster is recorded for on a part of FAT entry. A danger that data will be read unjustly can be lowered in analyzing a bit pattern which reduces continuity on a recording medium when recording data, carries out direct access to a user area as a result, and is recorded on a user area.
[0046]In this invention of (5), there are simplicity of structure where it is the same as processing of the above (1) thru/or an invention of (3) except recording a defect region at the time of medium initialization, and a merit that processing is light.
[0047]According to this invention, it is (6) in order to solve an aforementioned problem. Said recording device, A random data generation means which generates random data using an optional parameter, A random data writing means which writes random data obtained by said random data generation means in the whole user area of said portability type recording medium when initializing said portability type recording medium, A data recorder given in (1) having a parameter recording device which records said parameter on a system management area of said portability type recording medium is provided.
[0048]According to this invention, it is (7) in order to solve an aforementioned problem. Said random data writing means, When deleting data from said portability type recording medium, a data recorder given in (6) being what writes said random data in a data deletion field of said portability type recording medium again is provided.
[0049]A 2nd embodiment that mentions this invention of (6) and (7) later corresponds, and related figures are drawing 20 thru/or drawing 22.
[0050](Operation effect) At the time of initialization (shipment) of a portability type recording medium, a user area usually serves as a uniform value (each BITSUTO **, wholly ON, or wholly OFF).
[0051]Therefore, when only a small number of data is recorded on a portability type recording

medium, since the number of combination decreases to a round robin attack which was described by the invention of the above (4), a degree of the safety of data becomes low.
[0052]However, according to this invention of (6) and (7), a user area of a portability type recording medium, Since ON/OFF of a bit of a field which is not recorded is not uniform even when only a small number of data is recorded on a medium, since a value random at the time of initialization of a portability type recording medium is recorded, in order to attack, the round robin technique is needed, and the safety of data improves.
[0053]According to this invention, it is (8) in order to solve an aforementioned problem. Said recording device, A random data generation means which generates random data using an optional parameter, A data recorder given in (1) having a free-space selecting means which makes multiple selection of the intact field from a user area of said portability type recording medium, and a random data writing means which writes said random data in a field obtained by said free-space selecting means is provided.
[0054]A 2nd embodiment that mentions this invention of (8) later corresponds, and related figures are drawing 20 and drawing 23.
[0055](Operation effect) If it means altering data before writing data in a user area of a portability type recording medium, A bit pattern of a user area before writing in data is all dumped, and is recorded, and if all bit patterns of a user area are dumped again, both bit patterns are compared and difference is taken after writing in, pinpointing of a field where written-in data is recorded will be able to be performed.
[0056]Therefore, when only a small number of data is recorded on a portability type recording medium, since the number of combination decreases to a round robin attack which was described by the invention of the above (4), a degree of the safety of data becomes low.
[0057]However, according to this invention of (8), when writing data in a user area of a portability type recording medium, the safety of data improves to the above-mentioned attack by writing in with data to actually record dummy data on simultaneously.
[0058]According to this invention, it is (9) in order to solve an aforementioned problem. Said recording device, unit recording areas where said user area continues said data for users -- therefore, it recording continuously and with unit-recording-areas ID at the tail end in a head among said continuous unit recording areas. ID recording device which records defect region ID in said unit recording areas on a table for file management of said system management area, A data recorder given in (1) having an address means to ask for a physical address of said data for users recorded on said portability type recording medium, based on ID recorded on said table for file management is provided.
[0059]A 2nd embodiment that mentions this invention of (9) later corresponds, and related figures are drawing 24 and drawing 25.
[0060](Operation effect) For example, generally size of data photoed with a high definition digital camera etc. is large, therefore the number of a FAT entry used when recording the shot data on a portability type recording medium also becomes large.
[0061]As mentioned above, when recording data of 6 megabytes (equivalent to both incompressible image data 2 million ****) of DISUKUHE with a cluster size of 16 K bytes, 375 FAT entries are needed.
[0062]And if an entry of FAT becomes large, a burden of the encryption/decoding processing in the above (1) thru/or an invention of (3) will become large.
[0063]On the other hand, it is also possible for recording information which a head position in which data is written, and a position at the tail end understand on a system management area, when recording data to access data.
[0064]In this case, since that position and number must be recorded if a defective cluster is all over a field which records data, although the number of required FAT entries can be managed with a minimum of two pieces, the number of that much required entries increases, but. Usually, the number of FAT entries required [since it is almost zero] when writing one picture in a user area is three, information which a head position in which data is written, and a position at the tail end understand, and information showing the number of a defective cluster which exists in a field to write in.

[0065]Therefore, when writing in 6 megabytes of the above-mentioned data, 1/100 or less is the number of a needed FAT entry.
[0066]This serves as a very effective means for improvement in processing speed of encryption/decryption of a data reproduction apparatus.
[0067]According to this invention, it is (10) in order to solve an aforementioned problem. Said recording device, A processing means for said data for users to receive in part at least, and to perform predetermined processing, Information relevant to an address on data of a field where predetermined processing was performed by said processing means, and this address, and a processing information storage means to record at least one of parameters required for said predetermined processing on said data for system managements, A ****(ing) data recorder given in (9) is provided.
[0068]A 2nd embodiment that mentions this invention of (10) later corresponds, and related figures are drawing 24 thru/or drawing 27.
[0069]According to this invention, it is (11) in order to solve an aforementioned problem. A data recorder given in (10), wherein said processing means shuffles by a data unit in each unit recording areas is provided.
[0070]A 2nd embodiment that mentions this invention of (11) later corresponds, and related figures are drawing 24 thru/or drawing 28, and drawing 30.
[0071]According to this invention, it is (12) in order to solve an aforementioned problem. A data recorder given in (10), wherein said processing means shuffles in each unit-recording-areas unit is provided.
[0072]A 2nd embodiment that mentions this invention of (12) later corresponds, and related figures are drawing 24 thru/or drawing 29.
[0073]According to this invention, it is (13) in order to solve an aforementioned problem. A data recorder given in (10), wherein said processing means performs a shuffle of to said whole data for users is provided.
[0074]A 2nd embodiment that mentions this invention of (13) later corresponds, and related figures are drawing 24 thru/or drawing 28, and drawing 31.
[0075]According to this invention, it is (14) in order to solve an aforementioned problem. A data recorder given in (10), wherein said processing means performs processing which enciphers data is provided.
[0076]A 2nd embodiment that mentions this invention of (14) later corresponds, and related figures are drawing 24 thru/or drawing 27, and drawing 32.
[0077]According to this invention, it is (15) in order to solve an aforementioned problem. Said processing means, a unit -- a field -- inside -- a shuffle -- unit recording areas -- a unit -- a shuffle -- said -- a user -- ** -- data -- the whole -- receiving -- a shuffle -- and -- data encryption -- processing -- inside -- from -- at least -- two -- a ** -- processing -- combining -- carrying out -- things -- the feature -- carrying out -- (-- ten --) -- a statement -- a data recorder -- providing -- having .
[0078]A 2nd embodiment that mentions this invention of (15) later corresponds, and related figures are drawing 24 thru/or drawing 28 and drawing 30, and drawing 32.
[0079](Operation effect) It is premised on recording data continuously on a user area in an invention of the above (9).
[0080]Therefore, the way things stand, it is analyzing a bit pattern which carries out direct access to a user area, and is recorded on a user area, and there is a possibility of reading unjustly the contents of data currently recorded there.
[0081]then, when recording data in an invention of (10), processing which comes out of what it does not record as it is, but it processes shuffling data or enciphering etc. and is recorded, and improves the safety of data is performed.
[0082]In this case, if it is embedded into a FAT entry of an invention of the above (9) as a parameter required for processing of a shuffle or encryption is shown in drawing 26, It becomes possible to add various processing variations for protecting data for every data, and an effect that size of FAT which is an effect of the invention of the above (9) can be made small can also be acquired.

[0083]An invention of (11) thru/or (15) performs processing for improving the safety of data.
[0084]According to this invention, it is (16) in order to solve an aforementioned problem. Said recording device, A data recorder given in (1) having a code extraction recording device which records a predetermined code produced by extracting from user data recorded on said portability type recording medium on said system management area is provided.
[0085]According to this invention, it is (17) in order to solve an aforementioned problem. Said data reproduction means for system managements, A code extraction means to extract a predetermined code from said data for users read from said portability type recording medium, A code extracted by this code extraction means, and said code which are extracted when recording said data for users on said portability type recording medium, and is beforehand recorded on said system management area Said code collation means to compare, A ****(ing) data reproduction apparatus given in (3) is provided.
[0086]A 2nd embodiment that mentions this invention of (16) and (17) later corresponds, and related figures are drawing 34 thru/or drawing 38.
[0087](Operation effect) Although it is possible for an invention of (18) which this (16) and (17) invent and mention later to having been the invention which secures the safety of data by carrying out the scramble of the data which the above (10) thru/or an invention of (15) record, being unable to read data, and carrying out to read data, When it alters, it is the invention which secures the safety of data by giving a mechanism in which it turns out that it altered.
[0088]In this case, as a fundamental view, it is based on a message attestation child's (Message Authentication Code:MAC) method used by communication etc.
[0089]Below, a method of this MAC is explained.
[0090]In a method of detecting an alteration of data using MAC, a code which performs a predetermined operation (a HASH function (hash value) which is a directivity function is usually used) to data, and is first called a message digest (MD) to it is taken out.
[0091]This MD has the feature of changing a lot, when the contents of the original data change from character of a HASH function.
[0092]Next, MD is enciphered using an encryption key severely protected from the 3rd person in a secret.
[0093]This enciphered MD is MAC and transmits this MAC to a communications partner with data at the time of communication.
[0094]In a side which received, a predetermined operation is first performed to data like **** from data, and MD is obtained.
[0095]Next, it decrypts using a key to decryption and MD' is obtained from MAC which received together.
[0096]Since it will become a different code from MD and MD' if data is altered in the middle of communication, existence of an alteration of data in the middle of communication can be investigated by comparing MD and MD'.
[0097]The above is the method of alteration detection of data based on MAC.
[0098]Incidentally, when enciphering MD, generally may call an electronic signature a case where MAC and a data source enciphered MD for a code using an algorithm of a common key encryption system using the same encryption/decryption key with a secret key by data source and a receiver, and a receiver decrypts it by a public key, but. In this invention, both will be generically called MAC.
[0099]In an invention of (16), when recording data on a user area by a technique by invention of (9), MD is calculated first.
[0100]Then, as shown in drawing 35, MD (hash value) is recorded for this MD into a FAT entry of an invention of (9).
[0101]Usually, in the case of MAC, communication etc. need to encipher MD as not being altered in the middle of.
[0102]However, intermediary **** [as] as which the whole system management area is enciphered as a premise in this invention.
[0103]Therefore, even if it records MD on a FAT entry which is in a system management area without enciphering especially, the same effect as MAC can be acquired.

[0104]In this invention, an effect of becoming possible to read data with the same processing speed as an invention of the above (3) by forming the mode which passes processing of alteration detection is acquired.
[0105]An invention of (17) performs collation processing for alteration detection using MD (hash value) recorded by invention of the above (16), and is applied to a data reproduction apparatus by invention of the above (3).
[0106]According to this invention, it is (18) in order to solve an aforementioned problem. Said data reproduction means for system managements, A parameter reading means which reads said parameter from said system management area, A data reproduction apparatus given in (3) having a means to compare random data generated using a parameter read from said system management area and random data indicated to a cluster of a free space of said portability type recording medium is provided.
[0107]A 2nd embodiment that mentions this invention of (18) later corresponds, and related figures are drawing 20 thru/or drawing 22.
[0108](Operation effect) This invention of (18) is a data reproduction apparatus for reading data recorded with a data recorder of an invention of the above (6) and (7).
[0109]Even when a malicious user eliminates data unjustly using other recorders according to this invention of (18), An effect that it can leave a trace of having eliminated data unjustly is acquired from a bit pattern of an eliminated user area differing from a pattern recorded by invention of the above (6) and (7).
[0110]
[Embodiment of the Invention]With reference to drawings, an embodiment of the invention is described below.
[0111](A 1st embodiment) A 1st embodiment of the data recording/playback equipment by this invention is first described using drawing 1, drawing 3, drawing 4, drawing 6, or drawing 10.
[0112]The portion to which the same number was assigned in each of these figures shall have the same function.
[0113]Drawing 1 is a block diagram showing the composition of the data storage/playback equipment in a 1st embodiment.
[0114]Namely, this data storage / playback equipment 101, PC110 of the exterior, and the communications department 102 which performs communication, It comprises the operating memory part 103 connected to this communications department 102 via the internal bus, respectively, the memory part 104 for key data memory, the control section 105, the decoding section 106, the encryption section 107, the portability type storage actuator 108, and the medium judgment part 109.
[0115]The communications department 102 SCSI (Small Computer SystemInterface) and Ethernet, It has a function which carries out the exchange of the data creation and the editing device and data of PC110 of data recording / playback equipment exterior, a workstation, etc., or a command using radio, such as telecommunication cables, such as a serial cable, or infrared rays.
[0116]The operating memories 103 are data sent by the communications department 102 etc. and a memory for buffering gradual data in the middle of various processing, and loading a program.
[0117]The memory part 104 for key data storing is a memory for storing encryption keys, such as confidential information, for example, DES etc.
[0118]The control section 105 is a portion which controls the whole processing of data storage / playback equipment 101.
[0119]The decoding section 106 reads the information for decrypting data from the memory part 104 for key data storing, and decrypts data.
[0120]Similarly, the encryption section 107 reads the information for enciphering data from the memory part 104 for key data storing, and enciphers data.
[0121]The portability type storage actuator 108 performs read-out/writing of the data of the field on the portability type storage 100 with which data storage / the playback equipment 101 concerned are loaded (elimination is included) according to the processing demand from the

control section 105.
[0122]The medium judgment part 109 judges whether the storage with which data storage / the playback equipment 101 concerned are loaded is the portability type storage 100 currently recorded by the technique by this invention, or it is the other storage.
[0123]Drawing 3 is a figure for explaining a general file system, and shows the composition on the storage 1 of the FAT filesystem used by Windows or MS-DOS here.
[0124]Generally in the storage 1 of a FAT filesystem. as the system management area 7 -- a boot sector (0EM ID and a loader routine.) Comprise BPB on which the information about a device is recorded and 2 which consists of reserved areas, FAT3, the copy 4 of FAT, and the entry table 5 of the root directory, and. It comprises the file area 6 as the user area 8 (it is the following literature for details reference: "MS-DOS encyclopedia Volume1" and ASCII publication office (1989) p112-118).
[0125]On the other hand, drawing 4 shows the composition on the portability type storage 100 used by a 1st embodiment by this invention.
[0126]In drawing 4, the data of the system management area 7 is the same key data as the enciphered key data stored in the memory part 104 for key data storing of drawing 1, and is enciphered and recorded by the same method as the method of enciphering the encryption section 107.
[0127]Drawing 6 is a flow chart which shows the flow of the processing at the time of the data read in a 1st embodiment by this invention.
[0128]When reading data from the portability type storage 100, According to the data read demand (Step S1) on the portability type storage 100 from external PC110 grade, First, the data for system managements which is enciphered by the system management area of the portability type storage 100, and is recorded on it is read to the operating memory 103 using the portability type storage actuator 108 (Step S2).
[0129]Then, the read data for system managements which is enciphered is decrypted using the decoding section 106 (Step S3), and the data for system managements is obtained.
[0130]If the data for system managements is obtained, the data which read the appointed data using the information (step S4), and was read to PC110 of the exterior via the communications department 101 will be transmitted, and it will end (Step S5).
[0131]Drawing 7 is a flow chart which shows the flow of processing when accessing for the first time to the portability type storage 100 by a 1st embodiment and reading data.
[0132]When accessing for the first time to the portability type storage 100 and reading data, according to the data read demand (Step S21) on the portability type storage 100 from external PC110 grade, it is judged first whether access is the first (Step S22).
[0133]And access reads the data for system managements which is enciphered by the system management area of the portability type storage 100, and is recorded on it to the operating memory 103 using the portability type storage actuator 108 at a certain time for the first time (Step S23).
[0134]Then, the read data for system managements which is enciphered is decrypted using the decoding section 106 (Step S24), and the data for system managements is obtained.
[0135]If the data for system managements is obtained, the data which read the appointed data using the information (Step S25), and was read to PC110 of the exterior via the communications department 102 will be transmitted, and it will end (Step S26).
[0136]However, in Step S22, when access is not the first. The data which carried out through [of the above-mentioned step S23 and the processing of S24], read the appointed data using the information on the data for system managements obtained in front (Step S25), and was read to PC110 of the exterior via the communications department 102 is transmitted, and it ends (Step S26).
[0137]Drawing 8 is a flow chart which shows the flow of processing when writing in data by a 1st embodiment.
[0138]In writing the data received from external PC100 via the communications department 102 in the portability type storage 100, it reads the data for system managements to the operating memory 103 in the same procedure as the time of read-out first (Step S40, S41).

[0139]Then, the data received from external PC100 is written in the portability type storage 100 using the decrypted data for system managements (Step S42, S43).
[0140]Since the composition of the data on the portability type storage 100 is updated at this time, naturally the data for the system managements on the operating memory 103 is also updated (Step S44).
[0141]Then, the data for the system managements on the operating memory 103 is enciphered using the encryption section 107 (Step S45), The data for system managements which enciphered [above-mentioned] using the portability type storage actuator 108 is written in the system management area of the portability type storage 100 (Step S46), and it ends (Step S47).
[0142]Drawing 9 is a flow chart which shows the flow of processing when accessing for the first time to the portability type storage 100 by a 1st embodiment and writing in data.
[0143]When accessing for the first time to the portability type storage 100 and writing in data, according to the data writing demand (Step S60) on the portability type storage 100 from external PC110 grade, it is judged first whether access is the first (Step S61).
[0144]And access reads the data for system managements which is enciphered by the system management area of the portability type storage 100, and is recorded on it to the operating memory 103 using the portability type storage actuator 108 at a certain time for the first time (Step S62).
[0145]Then, the data received from external PC100 is written in the portability type storage 100 using the decrypted data for system managements (Step S63, S64).
[0146]Since the composition of the data on the portability type storage 100 is updated at this time, naturally the data for the system managements on the operating memory 103 is also updated (Step S65).
[0147]Then, the data for the system managements on the operating memory 103 is enciphered using the encryption section 107 (Step S66), The data for system managements which enciphered [above-mentioned] using the portability type storage actuator 108 is written in the system management area of the portability type storage 100 (Step S67), and it ends (Step S68).
[0148]However, in Step S61, when access is not the first. Through [of the above-mentioned step S62 and the processing of S63] is carried out, and the data received from external PC100 is written in the portability type storage 100 using the information on the data for system managements obtained in front (Step S63, S64).
[0149]Since the composition of the data on the portability type storage 100 is updated at this time, naturally the data for the system managements on the operating memory 103 is also updated (Step S65).
[0150]Then, the data for the system managements on the operating memory 103 is enciphered using the encryption section 107 (Step S66), The data for system managements which enciphered [above-mentioned] using the portability type storage actuator 108 is written in the system management area of the portability type storage 100 (Step S67), and it ends (Step S68).
[0151]That is, it will encipher each time and the data for system managements will be written in the system management area of the portability type storage 100.
[0152](a) of drawing 10 is other flow charts which show the flow of processing when accessing for the first time to the portability type storage 100 by a 1st embodiment and writing in data.
[0153]When accessing for the first time to the portability type storage 100 and writing in data, according to the data writing demand (Step S80) on the portability type storage 100 from external PC110 grade, it is judged first whether access is the first (Step S81).
[0154]And access reads the data for system managements which is enciphered by the system management area of the portability type storage 100, and is recorded on it to the operating memory 103 using the portability type storage actuator 108 at a certain time for the first time (Step S82).
[0155]Then, the data received from external PC100 is written in the portability type storage 100 using the decrypted data for system managements (Step S83, S84).
[0156]Since the composition of the data on the portability type storage 100 is updated at this time, naturally the data for the system managements on the operating memory 103 is also updated and (Step S85) ended (Step S86).

[0157]However, in Step S81, when access is not the first. Through [of the above-mentioned step S82 and the processing of S83] is carried out, and the data received from external PC100 is written in the portability type storage 100 using the information on the data for system managements obtained in front (Step S84).
[0158]Since the composition of the data on the portability type storage 100 is updated at this time, naturally the data for the system managements on the operating memory 103 is also updated and (Step S85) ended (Step S86).
[0159](b) of drawing 10 is a flow chart which shows the flow of processing when there is a discharge demand of the portability type storage 100 by a 1st embodiment.
[0160]Namely, when there is a discharge demand of the portability type storage 100. After enciphering the data for system managements (Step S91) and recording this enciphered data for system managements on the system management area on the portability type storage 100 (Step S92), the portability type storage 100 is discharged (Step S93).
[0161]That is, only when discharging the portability type storage 100 from the data recording / playback equipment 101 by this invention, the data for system managements is enciphered and it records on the system management area on the portability type storage 100.
[0162]Although all the data of a system management area is enciphered, it may be made to encipher only the copy of FAT and FAT, and the entry table of a root directory in the above explanation, as shown in drawing 5.
[0163]Although the explanation so far explained PC to the example as an external device of a data recorder, as an external device, it is not limited to this.
[0164]For example, it does not matter even if it may be information editing equipment, such as a workstation and PDA, instead of PC or is an image imaging device like a scanner, a digital camera, and a digital camcorder.
[0165]Naturally various kinds of modification and change are possible for each composition of this embodiment of the invention.
[0166]As shown in drawing 2, as the image imaging device 130, While comprising the optical system 120, the image pick-up part 121, the A/D conversion part 122, the image processing portion 123, the format conversion part 124, and the user interface part 125, It comprises the operating memory part 103 which is a component as data recording / playback equipment 101, the memory part 104 for key data memory, the control section 105, the decoding section 106, the encryption section 107, the portability type storage actuator 108, and the medium judgment part 109.
[0167]The optical system 120 comprises a lens, a body tube drive system, etc., and carries out image formation of the image to the image pick-up part 121.
[0168]The image pick-up part 121 changes a lightwave signal into an electrical signal, and the data which carried out the A/D conversion of said electrical signal, and digitized it is stored in the operating memory part 103 in the A/D conversion part 122.
[0169]In the image processing portion 123, various processings (for example, adjustment of a white balance, gamma conversion, edge enhancement processing, etc.) for generating a picture are performed from the digital data stored in the aforementioned operating memory 103.
[0170]The format conversion part 124 is a portion which changes the data of the aforementioned picture into preservation format, such as JPEG.
[0171]The user-interface part 125 consists of user interfaces, such as a shutter, a liquid crystal finder, and a button for various photographing mode setting out.
[0172]The demand of elimination of a file, etc. is also inputted via the user-interface part 125.
[0173]The above composition of the inside of the dotted line of drawing 2 is the same as that of the data recording/playback equipment of a 1st embodiment so that drawing 2 may show.
[0174]The portion which was considering the exchange of data as external PC110 grade through the communications department 102 in the case of a 1st embodiment only replaced exchanging data between the dotted-line exteriors in an image imaging device in drawing 2.
[0175]Therefore, also in composition like drawing 2, it is possible to have a function of a 1st embodiment.
[0176]The privacy of a data content and bona fides are secured for mass data like a picture, and

the above composition enables it to provide the data recorder which can record data at high speed.
[0177]And the following inventions are included in a 1st embodiment that was mentioned above.
[0178](1) In the data recording/playback equipment which records data on a portability type storage, A means to hold confidential information in a device, and a means to perform encryption and decryption using said confidential information, A means to encipher some of data for system managements of said portability type medium, or data for system managements, and to record on the system management area of said portability type storage using said encoding means, Said said enciphered data for system managements is read from the system management area of said portability type storage, Data recording/playback equipment having a means to decrypt some of said enciphered data for system managements, or data for system managements which were enciphered using said decoding means.
[0179](2) Data recording/playback equipment, wherein said data recording/playback equipment process said encryption in parallel to the time of performing processing which writes data in the user area of said portability type storage in time.
[0180]In the technique by (2nd embodiment) and a 1st embodiment that was mentioned above in time, the data on a portability type recording medium is dumped, and there is a risk of having a possibility that a data content will be read by the inaccurate attack method of changing a reading position one by one.
[0181]In the case of a recording medium which stores the picture especially photoed with the digital camera. The kind (the format of "WORD", "excel", "text", "jpeg", "tiff", "mpeg", etc., etc.) of data to photo was also decided (JPEG, TIFF, FlashPix, etc.), Since data size is also almost more nearly constant still when the pixel number of CCD is immobilization, in the technique by a 1st embodiment, there is a difficulty that it is weak, to the above unjust attacks.
[0182]So, in this 2nd embodiment, it has intention of providing the data recording/playback equipment accompanied by the measure against defense to such an unjust attack.
[0183]First, the term used by this 2nd embodiment is explained.
[0184]
(1) Logically accessible physically accessible unit field = cluster (2) sector [unit field =] (3) FAT : It is an abbreviation of File Allocation Table and is a file system name of MS-DOS. Although FAT is used in the following explanation like the general term of the management table which a file system uses, "FAT" is a name of the management table used with the file system used by MS-DOS or Windows until it gets tired.
(4) false defect cluster: -- or [that have not necessarily actually broken physically and it is normal] -- the cluster (definition within this specification) made into the defect by operating the contents of the management table showing whether it is a defect.
(5) Pseudo-random : The word "false" is attached in order to generate a random number using a pseudo-random number series.
[0185]Next, the outline of a 2nd embodiment is explained.
[0186]According to this 2nd embodiment, it roughly divides enciphering a system management area (FAT is included) into a base, and the following five techniques are contained in it.
[0187](1) Make physical arrangement of the cluster to data pseudo-random (continuity is abolished).
[0188](2) Make a false defect cluster and make read-out of data difficult.
[0189]It is subordinate to the above (1) and (2), and it has the following cases.
[0190]a) Initialize a user area by pseudo-random data at the time of data initialization.
[0191]b) Transpose the field to the original random data at the time of data deletion.
[0192]This is for considering it as those of an alteration with doubt, when there is a cluster on which data which is intact and is different from the time of initialization was recorded.
[0193](3) Also write fake data in a free space (the above-mentioned false defect cluster region is also included) of recording media, such as an MO disk, simultaneously at the time of data writing.
[0194]This (3) is boiled, therefore the above (1), (2), and concomitant use are possible for it.
[0195](4) Use that the size of data without the postscript to data is almost constant, and realize

small-scale-ization (the operation amount of FAT encryption is reduced) of FAT.
[0196]It is subordinate to this (4), and there are the following cases.
[0197]a) Perform various processing of shuffling at the time of data recording.
[0198]b) Record the parameter of processing on the amount region of a system management.
[0199](5) At the time of data recording, calculate the hash value (OR Error Correcting Code/Error Detecting Code) of data, and record on a system management area.
[0200]Drawing 11 is a figure for explaining the file management technique of MS-DOS FAT16 file system corresponding to the five techniques of the above of a 2nd embodiment based on the above outlines.
[0201]That is, drawing 11 takes access to the file of file name file.text for an example.
[0202]In this case, the directory entry (FAT16) of file.text as shown according to menu form in drawing 11 is looked for by searching the entry (or entry of a subdirectory) of a root directory.
[0203]Here, the case where a FAT entry (ID) is 14 as a start cluster (ID) is shown.
[0204]If the size of a file as shown according to menu form in drawing 11 is 4800bytes, for example, is 1 cluster =1024bytes, it shows the case where five clusters are needed.
[0205]Here, the case where it is 1 cluster =2 sector =1024bytes is shown.
[0206]"H" in drawing 11 shall mean a hexadecimal number.
[0207]And a FAT entry (ID) receives 11, 12, 13, 14, 15, 16, 17, 18, 19, and 20, Each cluster CH, DH, FFFFH, FH, 10H and 12H, FFF7H, 13H, FFFFH, and 0H are the examples by the above-mentioned pseudo-random one which are randomized and are assigned, respectively.
[0208]In this example, it comes to be below the FAT link of one data.
[0209]First, access is started for a FAT entry (ID) from 14 as a start cluster (ID), A FAT entry (ID) shifts to 15 in FH=15, a FAT entry (ID) shifts to 16 in 10H=16, a FAT entry (ID) shifts to 18 in 12H=18, and a FAT entry (ID) shifts to 19 in 13H=19.
[0210]Since a FAT entry (ID) is a poor cluster as the above-mentioned false defect cluster region FFF7H of 17, in the FAT entry (ID), the FAT entry (ID) has shifted to 18 from 16.
[0211]In FFF8 of 19 - FFFFH, a FAT entry (ID) is a cluster of the last of a file.
[0212]And a FAT entry (ID) is an intact cluster 0H of 20.
[0213]Next, each example corresponding to the five techniques of the above of a 2nd embodiment based on the above outlines is explained with reference to drawing 12 thru/or drawing 37.
[0214]The portion to which the same number as a 1st embodiment mentioned above in each of these figures was assigned shall have the same function.
[0215](The 1st example) The 1st example of a 2nd embodiment of the data recording/playback equipment by this invention is first explained using drawing 12 thru/or drawing 17.
[0216]Drawing 12 is a block diagram showing the composition of the data recording/playback equipment by the 1st example in a 2nd embodiment.
[0217]Namely, this data storage / playback equipment 101, PC110 of the exterior, and the communications department 102 which performs communication, The operating memory part 103 connected to this communications department 102 via the internal bus, respectively, the memory part 104 for key data memory, the control section 105, the decoding section 106, the encryption section 107, the portability type storage actuator 108, the medium judgment part 109 (not illustrating refer to a 1st embodiment), It comprises the data division part 201 and the cluster selecting part 202.
[0218]The communications department 102 SCSI (Small Computer SystemInterface) and Ethernet, It has a function which carries out the exchange of the data creation and the editing device and data of PC110 of data recording / playback equipment exterior, a workstation, etc., or a command using radio, such as telecommunication cables, such as a serial cable, or infrared rays.
[0219]The operating memories 103 are data sent by the communications department 102 etc. and a memory for buffering gradual data in the middle of various processing, and loading a program.
[0220]The memory part 104 for key data storing is a memory for storing encryption keys, such as confidential information, for example, DES etc.

[0221]The control section 105 is a portion which controls the whole processing of data storage / playback equipment 101.
[0222]The decoding section 106 reads the information for decrypting data from the memory part 104 for key data storing, and decrypts data.
[0223]Similarly, the encryption section 107 reads the information for enciphering data from the memory part 104 for key data storing, and enciphers data.
[0224]The portability type storage actuator 108 performs read-out/writing of the data of the field on the portability type storage 100 with which data storage / the playback equipment 101 concerned are loaded (elimination is included) according to the processing demand from the control section 105.
[0225]In the medium judgment part 109 which is not illustrated, it is judged whether the storage with which data storage / the playback equipment 101 concerned are loaded is the portability type storage 100 currently recorded by the technique by this invention, or it is the other storage.

[0226]The data division part 201 divides data into the size of an accessible unit field logically on the portability type recording medium 100.
[0227]The cluster selecting part 202 chooses logically the cluster which is not used from the portability type recording medium 100 in accordance with the predetermined rule as a cluster of an accessible unit field.
[0228]Namely, the data recording/playback equipment by this 1st example, In the data recording/playback equipment by a 1st embodiment that was mentioned above, In the processing which records data on the portability type recording medium 100, the data division part 201 divides data into the size of an accessible unit field logically on the portability type recording medium 100, and. By choosing logically the cluster which is not used by the cluster selecting part 202 from the portability type recording medium 100 in accordance with the predetermined rule as a cluster of an accessible unit field, According to the processing demand from the control section 105, said divided data is logically characterized by said thing [having been chosen] recorded on the cluster of an accessible unit field one by one.
[0229]Namely, when recording data on the disks as a portability type recording medium (for example, MO etc.), are trying for a cluster to usually record data on the field connected continuously, but. There is a threat that the data written in the disk is read by dumping the user area of a disk one by one, in case of this method.
[0230]So, with the data recording/playback equipment by this 1st example, when writing in data, the technique of avoiding the above-mentioned threat shall be adopted by choosing the cluster which dares to be discontinuous and writing in data.
[0231]For example, in the case of the disk size 1G and the image size 6M (incompressible 2 million pixels), there are 375 cluster numbers for the cluster number of an entire disk to record those with 62500 piece and one image data also in the case where the size of a cluster is 16K.
[0232]If the technique by the 1st example is adopted to such a disk, when a system management area is enciphered and the link between clusters is not known, The data recorded by 375 clusters in right turn from 62500 clusters also for restoring image data by groping (since random data was written in all the fields of De Dis . KU at the time of initialization) must be read, A decipherment becomes fairly difficult (there is combination as about 62500^{375} by simple calculation).
[0233]They are temporarily dumped by all the recording-medium fields of the back before writing in data, and by [said / two / which carry out a data comparison] having been dumped, Since the turn of the data for reading data is not known even if the field where data is recorded is revealed, it is 375! It is necessary to decode true data from the combination of a passage.
[0234]Actually, in the case of image data, it is 375 from the information on frequency, hue Seki, etc.! Although it is possible to narrow a search range to a slight degree from a passage, it can be said that the decipherment itself is next to impossible.
[0235]And in the technique by this 1st example, since the physical continuity of a cluster is lost, a reading speed falls, but it is fundamentally the same as the usual file stem, and the data size of

a system management area does not change.
[0236]Drawing 13 shows the data management gestalt in FAT16 file system based on the technique by this 1st example.
[0237]That is, drawing 13 takes out and shows a cluster portion from drawing 11 which explained the outline of a 2nd embodiment previously, and is proportionate to drawing 11 except not having provided the false defect cluster region.
[0238]In this example, it comes to be below the FAT link of one data.
[0239]First, access is started for a FAT entry (ID) from 14 as a start cluster (ID), A FAT entry (ID) shifts to 15 in FH=15, a FAT entry (ID) shifts to 16 in 10H=16, a FAT entry (ID) shifts to 17 in 11H=17, and a FAT entry (ID) shifts to 18 in 12H=18.
[0240]In FFFFH of 18, a FAT entry (ID) is a cluster of the last of a file.
[0241]Drawing 14 shows in reference the example in case data is recorded on the user area of the portability type recording medium which has a system management area and a user area, when the usual file system is used.
[0242]In this case, in the portability type recording medium, as physical arrangement of data, the cluster region of ID(address) =2 – 37 is arranged, for example so that the physical possible continuity may be secured.
[0243]And in this drawing 14, the example by which data is written in the cluster region of ID (address) =14 which has hatching – 18 is shown.
[0244]Drawing 15 shows the recording form of data based on the technique by this 1st example.
[0245]That is, in this drawing 15, first, the data to record is divided into the size of a cluster and shows respectively what is recorded on the cluster region of cluster ID(address) =2 [selected at random], 3, 4--12, 13, 14--17, 18, and 19--33.
[0246]Drawing 16 matches the FAT link of one data in the case of being based on this 1st example with a part of drawing 14, and shows it.
[0247]As this drawing 16 shows, it is a technique which can be fundamentally treated by a FAT system.
[0248]Drawing 17 shows the example in case data is recorded on the user area of the portability type recording medium which has a system management area and a user area, when the file system by this 1st example is used.
[0249]In this case, in the portability type recording medium, as physical arrangement of data, the cluster region of ID(address) =2 – 37 is randomized and arranged, for example so that the physical possible continuity may be abolished.
[0250]And in this drawing 17, the example by which data is written in ID(address) =3 which has hatching, 12, 14, 17 and 19, and 33 cluster regions is shown.
[0251]The 2nd example of a 2nd embodiment of the data recording/playback equipment by this invention is explained using the (2nd example) next drawing 18, and drawing 19.
[0252]Drawing 18 is a block diagram showing the composition of the data recording/playback equipment by the 2nd example in a 2nd embodiment.
[0253]Namely, this data storage / playback equipment 101, PC110 of the exterior, and the communications department 102 which performs communication, The operating memory part 103 connected to this communications department 102 via the internal bus, respectively, the memory part 104 for key data memory, the control section 105, the decoding section 106, the encryption section 107, the portability type storage actuator 108, the medium judgment part 109 (not illustrating refer to a 1st embodiment), It comprises the cluster selecting part 301 and the random number generation part 302.
[0254]The communications department 102 SCSI (Small Computer SystemInterface) and Ethernet, It has a function which carries out the exchange of the data creation and the editing device and data of PC110 of data recording / playback equipment exterior, a workstation, etc., or a command using radio, such as telecommunication cables, such as a serial cable, or infrared rays.
[0255]The operating memories 103 are data sent by the communications department 102 etc. and a memory for buffering gradual data in the middle of various processing, and loading a program.

[0256]The memory part 104 for key data storing is a memory for storing encryption keys, such as confidential information, for example, DES etc.
[0257]The control section 105 is a portion which controls the whole processing of data storage / playback equipment 101, and writing control of the defective cluster information mentioned later will be performed by this control section 105.
[0258]The decoding section 106 reads the information for decrypting data from the memory part 104 for key data storing, and decrypts data.
[0259]Similarly, the encryption section 107 reads the information for enciphering data from the memory part 104 for key data storing, and enciphers data.
[0260]The portability type storage actuator 108 performs read-out/writing of the data of the field on the portability type storage 100 with which data storage / the playback equipment 101 concerned are loaded (elimination is included) according to the processing demand from the control section 105.
[0261]In the medium judgment part 109 which is not illustrated, it is judged whether the storage with which data storage / the playback equipment 101 concerned are loaded is the portability type storage 100 currently recorded by the technique by this invention, or it is the other storage.

[0262]The cluster selecting part 301 is logically chosen from the portability type recording medium 100 as a cluster of an accessible unit field in accordance with a predetermined rule.
[0263]The random number generation part 302 generates the random number for generating the random data using the parameter which is optional as random data used for the writing control of the defective cluster information mentioned later.
[0264]Namely, the data recording/playback equipment by this 2nd example, In the data recording/playback equipment by a 1st embodiment that was mentioned above, In the processing which records data on the portability type recording medium 100, choose two or more accessible unit fields from said portability type recording medium 100 at random logically by the cluster selecting part 301 and the random number generation part 302, and. It is characterized by registering with said data for system managements by making an accessible unit field into a defect region logically on said portability type recording medium 100 by the control section 105.
[0265]And in this 2nd example, it is characterized by making a false defect cluster at random on the portability type recording medium 100 at the time of initialization.
[0266]With a false defect cluster here, the cluster of a user area is not actually destroyed but the information that the cluster corresponding to a FAT entry has broken is only recorded (since the data for system managements is enciphered, nobody understands this information).
[0267]As for the data written in a recording medium, the false defect sector has entered some places of true data.
[0268]For example, when 10% of all the clusters are false defect sectors, on condition of the precedent, 38 false defect clusters (false data) will be contained in the cluster of an individual (375+38).
[0269]Therefore, in order to read data, it is necessary to discover the field where data is recorded and to remove the portion of a false defect cluster further after that from the 62500 whole cluster.
[0270]They are temporarily dumped by all the recording-medium fields of the back before writing in data, and by [said / two / which carry out a data comparison] having been dumped, Even if the field where data is recorded is revealed, it is possible to protect a data content toughly by using together with the technique by the 6th thru/or the 11th example mentioned later.
[0271]Since the data itself currently recorded on each cluster does not express a direct image in the case of compressed images, such as JPEG, the thing in particular used together with the technique by the 6th thru/or the 11th example is unnecessary, and it is possible to protect a data content toughly only by the technique by this 2nd example.
[0272]In the technique by this 2nd example, futility will produce only the part of a false defect cluster in a disk area.
[0273]However, since it is recorded in a FAT entry as defective cluster information was shown in drawing 11 by the usual method in the case of this 2nd example, it is not necessary to record

defective cluster information (position) on a place except FAT separately specially.
[0274]And in the technique by this 2nd example, since it is the same as the usual file stem, mounting is fundamentally easy, and since the cluster which writes in data has continuity, there is an advantage that the drawing speed of data is quick.
[0275](a) of drawing 19 and (b) make the initialization status of the FAT link in usual, and the initialization status of a FAT link based on the technique by this 2nd example contrast, and are shown.
[0276]That is, as shown in (a) of drawing 19, there is no change in any way with the case usual in the initialization status of the FAT link in usual.
[0277]On the other hand, as shown in (b) of drawing 19, in the technique by this 2nd example, the code which shows at the place of FAT entry (ID) =12 and 17 that it is a becoming false defect cluster region FFF7H is attached.
[0278]The 3rd example of a 2nd embodiment of the data recording/playback equipment by this invention is explained using the (3rd example) next drawing 20 thru/or drawing 22.
[0279]Drawing 20 is a block diagram showing the composition of the data recording/playback equipment by the 3rd example in a 2nd embodiment.
[0280]Namely, this data storage / playback equipment 101, PC110 of the exterior, and the communications department 102 which performs communication, The operating memory part 103 connected to this communications department 102 via the internal bus, respectively, the memory part 104 for key data memory, the control section 105, the decoding section 106, the encryption section 107, the portability type storage actuator 108, the medium judgment part 109 (not illustrating refer to a 1st embodiment), It comprises the cluster collating part 401 and the random number generation part 402.
[0281]The communications department 102 SCSI (SmallComputer SystemInterface) and Ethernet, It has a function which carries out the exchange of the data creation and the editing device and data of PC110 of data recording / playback equipment exterior, a workstation, etc., or a command using radio, such as telecommunication cables, such as a serial cable, or infrared rays.
[0282]The operating memories 103 are data sent by the communications department 102 etc. and a memory for buffering gradual data in the middle of various processing, and loading a program.
[0283]The memory part 104 for key data storing is a memory for storing encryption keys, such as confidential information, for example, DES etc.
[0284]The control section 105 is a portion which controls the whole processing of data storage / playback equipment 101.
[0285]The decoding section 106 reads the information for decrypting data from the memory part 104 for key data storing, and decrypts data.
[0286]Similarly, the encryption section 107 reads the information for enciphering data from the memory part 104 for key data storing, and enciphers data.
[0287]The portability type storage actuator 108 performs read-out/writing of the data of the field on the portability type storage 100 with which data storage / the playback equipment 101 concerned are loaded (elimination is included) according to the processing demand from the control section 105.
[0288]In the medium judgment part 109 which is not illustrated, it is judged whether the storage with which data storage / the playback equipment 101 concerned are loaded is the portability type storage 100 currently recorded by the technique by this invention, or it is the other storage.

[0289]It is compared whether the random data generated using the parameter read from the system management area and the data of the cluster collating part 401 currently recorded on the cluster of a free space of said portability type recording medium are the same as that of the time of initialization so that it may mention later.
[0290]The random number generation part 402 generates the random number for generating the random data using the parameter which has optionality in the whole user area mentioned later as random data used for the writing control of said random data.

[0291]Namely, the data recording/playback equipment by this 3rd example, In the data recording/playback equipment by a 1st embodiment that was mentioned above, in the processing which records data on the portability type recording medium 100, since said portability type recording medium is initialized, Generate random data using the parameter which is optional by the random number generation part 402, and write said random data in the whole user area according to the processing demand from the control section 105, and. The random data generated using the parameter which read said parameter beforehand recorded on said system management area, and was read from said system management area by the cluster collating part 401, When comparing whether the data currently recorded on the cluster of a free space of said portability type recording medium is the same as the time of initialization and deleting data from said portability type recording medium according to the processing demand from the control section 105, It is characterized by writing pseudo-random data in the intact field of said portability type recording medium.
[0292]And the technique by this 3rd example is compensated with the technique by the 1st and 2nd examples mentioned above.
[0293]That is, when recording data on the disks as a portability type recording medium (for example, MO etc.), the disk with which data is not recorded can usually consider the case where the whole disk area is initialized by 0 (OFF).
[0294]In such a case, there is a threat that the field where data is recorded, and the field which is not carried out will be able to be immediately understood by dumping an entire disk, only by the technique by the 1st and 2nd examples mentioned above.
[0295]So, in the technique by this 3rd example, it is the technique of reducing the above-mentioned threat by initializing an entire disk with a random value beforehand.
[0296]After this technique records data, it is effective to the attack which **** a data content.
[0297]However, in the technique by this 3rd example, although there is no effect in the attack of taking the difference a data recording front and after record in any way, a measure to this attack can be coped with by the technique by the 4th example described below.
[0298]It has the knowledge about a file system, and there is a possibility that the user area of the initialized above-mentioned disk may be uniformly initialized by the malicious user 0 etc. using the means of a low with other data recorders.
[0299]So, in the technique by this 3rd example, it has a function which can confirm whether write the specific data (pseudo-random data) depending on a place in an intact field, and data is unjustly written in the user area.
[0300]For this reason, specifically in the technique by the 3rd example, a pseudo-random number product sequence and its kind (what calls it a parameter, and is enciphered and recorded on a SHISUAMU management domain here) are used.
[0301]That is, it is because it can be confirmed what kind of random number sequence was recorded on which cluster, or whether data is unjustly written in the user area as mentioned above since it understands if the kind of random number generation is known.
[0302]In eliminating a data file, it usually only makes a FAT link part corresponding from a FAT entry intact (0H), but if it does in this way, the above-mentioned technique is not employable.
[0303]Then, in the technique by this 3rd example, when it eliminates, it is made to make into the same value as the time of initialization the value of the cluster which that file was using using the kind of the above-mentioned random number.
[0304]Drawing 21 is a key map for explaining the technique by this 3rd example.
[0305]Drawing 22 is a flow chart for explaining the technique by this 3rd example.
[0306]That is, ID of a FAT entry is set to n, when setting to x said parameter beforehand recorded on the system management area, such n and x are inputted into a random data generating device, and the random data for one cluster is generated (Step S11, S12, S13).
[0307]And initialize a user area extensively with a random value by recording the random data for this one cluster on the n-th cluster in the user area of a portability type recording medium, and. It ends, after enciphering the data for system managements and recording on the system management area of a portability type recording medium (Step S14, S15, S16, S17).
[0308]The 4th example of a 2nd embodiment of the data recording/playback equipment by this

invention is explained using the (4th example), next drawing 23.
[0309]Drawing 23 is a flow chart for explaining the function of the data recording/playback equipment by the 4th example in a 2nd embodiment.
[0310]About the composition of the data recording/playback equipment by this 4th example, since it is the same as the composition of the data recording/playback equipment by the 3rd example mentioned above, that explanation shall be omitted.
[0311]Namely, the data recording/playback equipment by this 4th example, In the data recording/playback equipment by a 1st embodiment that was mentioned above, In the processing which records data on the portability type recording medium 100, random data is generated using the parameter which is optional by the random number generation part 402, It is characterized by writing said random data in the intact field which made multiple selection from the user area according to the processing demand from the control section 105.
[0312]And this 4th example is a technique of recording dummy data simultaneously (Steps S53-S57), when recording data on a disk (Step S51, S52), as shown in drawing 23.
[0313]That is, about simultaneous record of dummy data, when setting ID of a FAT entry to n, this n is inputted into a random data generating device, and random data is generated (Step S53, S54).
[0314]And an intact cluster region is chosen at random and it is random data to this selected cluster region N<=n (however, N) It ends, after making it record until it becomes the number of cluster regions which writes in random data, and enciphering the data for system managements and recording on the system management area of a portability type recording medium (Step S55, S56, S57, S58, S59).
[0315]In the technique by this 4th example, since it is enciphered as system management data showed a 1st embodiment, about dummy data being recorded together with true data, it cannot distinguish from a user.
[0316]Since dummy data uses a free space (a false defect cluster is included) with intact status, portability type recording-medium fields, such as a disk, are not made useless at all (since it does not record on FAT at all, it does not become a file).
[0317]The 5th example of a 2nd embodiment of the data recording/playback equipment by this invention is explained using the (5th example) next drawing 24, and drawing 25.
[0318]Drawing 24 is the figure showing FAT entry composition, in order to explain the function of the data recording/playback equipment by the 5th example in a 2nd embodiment.
[0319]This FAT entry (ID) composition has start cluster ID, the last cluster ID, the number of a defective cluster, ID of the defective cluster 1, ID of the defective cluster 2, etc., as shown in drawing 24.
[0320](a) of drawing 25 and (b) are figures which are made to contrast the FAT filesystem at the time of applying to the 1st example correspondingly, and the file system based on the technique by this 5th example, and are shown.
[0321]That is, as shown in (a) of drawing 25, at the FAT filesystem at the time of applying to the 1st example correspondingly, there is almost no change with the case of the 1st example.
[0322]On the other hand, as shown in (b) of drawing 25, in the technique by this 2nd example. In FAT entry (ID) =K-1, K, K+1, K+2, K+3, K+4, and K+5, as a start cluster (ID), access is started from K (14) and a FAT entry (ID) shifts to K+1 (15), K+2 (1), and K+3 (17).
[0323]About the composition of the data recording/playback equipment by this 5th example, since it is the same as the composition of the data recording/playback equipment by the 2nd example mentioned above, that explanation shall be omitted.
[0324]Namely, the data recording/playback equipment by this 5th example, In the data recording/playback equipment by a 1st embodiment that was mentioned above, In the processing which records data on the portability type recording medium 100, the field which records data on said system management area logically ID of an accessible head and unit field at the tail end, Record the information on the defect region in the continuation field which records said data on the table for file management, and. When [which receives the data on said portability type recording medium] reading and accessing writing etc., it is characterized by asking for the physical address on the portability type recording medium of data from said table for file

management.
[0325]And the technique by this 5th example is based on the viewpoint as shown below.
[0326]For example, a cluster number the size of the data is 6 M bytes, and required in the system of FAT16 if it is 2 million-pixel non compression data in the case of the data recorder of a digital camera, Becoming 367 pieces also considering a cluster size as 16 K bytes, 367x 2= 734 bytes of management data required to manage one graphics file is needed.
[0327]By the way, in a digital camera, processing which is usually later added to data is not performed, and one data is recorded succeeding the cluster which usually continues.
[0328]Therefore, it is possible to access data, if the information is recorded when it is not necessary to link all the FAT like [in the case of the usual FAT system] and there is a defective cluster in the middle of start ID (address) of a cluster, and the last ID.
[0329]In disks, such as the latest MO, since a defective cluster usually hardly exists, in the case of the above-mentioned example, a field required to manage a data file by the above-mentioned technique drops to 1/hundreds of FAT16 system.
[0330]Considering enciphering a system management area, by this system, it is thought that reduction of the data volume of a system management area is a means very effective in shortening of processing time.
[0331]Since it is conditions to use a continuous cluster, the technique by this 5th example is inapplicable to the technique by the 1st, 3rd, and 4th examples mentioned above.
[0332]The 6th thru/or the 11th example of a 2nd embodiment of (the 6th thru/or the 11th example) next drawing 26 thru/or data recording/playback equipment reach and according to this invention using drawing 32 is explained.
[0333]Each of this the 6th thru/or 11th example is subordinately applied to the technique by the 5th example mentioned above.
[0334]Namely, the technique by the 5th example that mentioned above this the 6th thru/or 11th example, it is the technique of being different in a file in the data which uses that data volume of a file system required to manage a data file can be lessened, and is written in the data of a file system it enables it to come out of, shuffle or encipher.
[0335]Drawing 26 is the figure showing FAT entry composition, in order to explain the function of the data recording/playback equipment by the 6th thru/or the 11th example in a 2nd embodiment in common.
[0336]This FAT entry (ID) composition has the number of start cluster ID, the last cluster ID, processing information, and a defective cluster, ID of the defective cluster 1, ID of the defective cluster 2, etc., as shown in drawing 26.
[0337]Drawing 27 is a flow chart for explaining the function of the data recording/playback equipment by the 6th thru/or the 11th example in a 2nd embodiment in common.
[0338]First, as shown in drawing 27, if data is inputted, this process flow will create data processing information, and will record it into FAT (Step S71, S72).
[0339]Next, input data is processed according to data processing information, and data is recorded on a portability type storage (Step S73, S74).
[0340]Next, it ends, after updating the information on FAT and a directory entry, and enciphering the data for system managements and recording data on a portability type storage (Step S75, S76, S77).
[0341]And the data recording/playback equipment by the 6th example, When performing processing which writes data in the user area of said portability type storage in the data recording/playback equipment by the 5th example that was mentioned above, perform predetermined processing to some of whole data or data, and. It is characterized by recording the information relevant to the address on the data of the field which performed said processing, or an address, and a parameter required for said processing on the data for system managements.
[0342]Drawing 28 is a block diagram showing the composition of the data recording/playback equipment by the 7th example in a 2nd embodiment.
[0343]Namely, this data storage / playback equipment 101, PC110 of the exterior, and the communications department 102 which performs communication, The operating memory part 103

connected to this communications department 102 via the internal bus, respectively, the memory part 104 for key data memory, the control section 105, the decoding section 106, the encryption section 107, the portability type storage actuator 108, the medium judgment part 109 (not illustrating refer to a 1st embodiment), It comprises the shuffle processing part 501.
[0344]The communications department 102 SCSI (Small Computer SystemInterface) and Ethernet, It has a function which carries out the exchange of the data creation and the editing device and data of PC110 of data recording / playback equipment exterior, a workstation, etc., or a command using radio, such as telecommunication cables, such as a serial cable, or infrared rays.
[0345]The operating memories 103 are data sent by the communications department 102 etc. and a memory for buffering gradual data in the middle of various processing, and loading a program.
[0346]The memory part 104 for key data storing is a memory for storing encryption keys, such as confidential information, for example, DES etc.
[0347]The control section 105 is a portion which controls the whole processing of data storage / playback equipment 101.
[0348]The decoding section 106 reads the information for decrypting data from the memory part 104 for key data storing, and decrypts data.
[0349]Similarly, the encryption section 107 reads the information for enciphering data from the memory part 104 for key data storing, and enciphers data.
[0350]The portability type storage actuator 108 performs read-out/writing of the data of the field on the portability type storage 100 with which data storage / the playback equipment 101 concerned are loaded (elimination is included) according to the processing demand from the control section 105.
[0351]In the medium judgment part 109 which is not illustrated, it is judged whether the storage with which data storage / the playback equipment 101 concerned are loaded is the portability type storage 100 currently recorded by the technique by this invention, or it is the other storage.

[0352]In the data recording/playback equipment by the 6th example that was mentioned above, the shuffle processing part 501 performs shuffle processing within a block as said predetermined processing.
[0353]And in the data recording/playback equipment by the 6th example that was mentioned above, the data recording/playback equipment by this 7th example are characterized by carrying out as said predetermined processing.
[0354]Drawing 29 is a figure shown in order to explain the function of the data recording/playback equipment by the 7th example in a 2nd embodiment.
[0355]Namely, in the technique by this 7th example. In the field in which the data of file file.text of the user area on the portability type storage 100 is recorded. He performs shuffle processing by a cluster unit, and is trying to record the information on shuffle processing, including parameter etc., for the processing information on the system management area on the portability type storage 100.
[0356]Drawing 30 is a figure shown in order to explain the function of the data recording/playback equipment by the 8th example in a 2nd embodiment.
[0357]Namely, although shuffle processing is performed like the technique by the 7th example mentioned above in the technique by this 8th example, In the field in which the data of file file.text of the user area on the portability type storage 100 is recorded in that case. He performs shuffle processing by a block unit within a cluster, and is trying to record the information on shuffle processing, including parameter etc., for the processing information on the system management area on the portability type storage 100.
[0358]And in the data recording/playback equipment by the 6th example that was mentioned above, the data recording/playback equipment by this 8th example are characterized by performing shuffle processing by a block unit as said predetermined processing.
[0359]Drawing 31 is a figure shown in order to explain the function of the data recording/playback equipment by the 9th example in a 2nd embodiment.

[0360]Namely, although shuffle processing is performed like the technique by the 7th example mentioned above in the technique by this 9th example, In the field in which the data of file file.text of the user area on the portability type storage 100 is recorded in that case. He performs shuffle processing to the whole data, and is trying to record the information on shuffle processing, including parameter etc., for the processing information on the system management area on the portability type storage 100.
[0361]And in the data recording/playback equipment by the 6th example that was mentioned above, the data recording/playback equipment by this 9th example are characterized by performing shuffle processing to the whole data as said predetermined processing.
[0362]Drawing 32 is a figure shown in order to explain the function of the data recording/playback equipment by the 10th example in a 2nd embodiment.
[0363]Namely, in the technique by this 10th example. In the field which does not perform shuffle processing like the technique by the 7th example mentioned above but in which the data of file file.text of the user area on the portability type storage 100 is recorded. He performs encryption processing to the whole data, and is trying to record the processing information on the system management area on the portability type storage 100 as information about an algorithm, including information on an encryption key, etc.
[0364]And in the data recording/playback equipment by the 6th example that was mentioned above, the data recording/playback equipment by this 10th example are characterized by performing encryption processing to the whole data as said predetermined processing.
[0365]And the data recording/playback equipment by the 11th example, In the data recording/playback equipment by the 7th thru/or the 10th example which was mentioned above, As said predetermined processing, it is characterized by combining shuffle processing, the shuffle processing to the whole data, and at least two processings or more in the encryption processing to the whole data at the shuffle processing within said block, and a block unit.
[0366]The 12th example of a 2nd embodiment of the data recording/playback equipment by this invention is explained using the (12th example) next drawing 33 thru/or drawing 38.
[0367]Drawing 33 is a block diagram showing the composition of the data recording/playback equipment by the 12th example in a 2nd embodiment.
[0368]Namely, this data storage / playback equipment 101, PC110 of the exterior, and the communications department 102 which performs communication, The operating memory part 103 connected to this communications department 102 via the internal bus, respectively, the memory part 104 for key data memory, the control section 105, the decoding section 106, the encryption section 107, the portability type storage actuator 108, the medium judgment part 109 (not illustrating refer to a 1st embodiment), It comprises the hash operation part 601.
[0369]The communications department 102 SCSI (Small Computer SystemInterface) and Ethernet, It has a function which carries out the exchange of the data creation and the editing device and data of PC110 of data recording / playback equipment exterior, a workstation, etc., or a command using radio, such as telecommunication cables, such as a serial cable, or infrared rays.
[0370]The operating memories 103 are data sent by the communications department 102 etc. and a memory for buffering gradual data in the middle of various processing, and loading a program.
[0371]The memory part 104 for key data storing is a memory for storing encryption keys, such as confidential information, for example, DES etc.
[0372]The control section 105 is a portion which controls the whole processing of data storage / playback equipment 101.
[0373]The decoding section 106 reads the information for decrypting data from the memory part 104 for key data storing, and decrypts data.
[0374]Similarly, the encryption section 107 reads the information for enciphering data from the memory part 104 for key data storing, and enciphers data.
[0375]The portability type storage actuator 108 performs read-out/writing of the data of the field on the portability type storage 100 with which data storage / the playback equipment 101 concerned are loaded (elimination is included) according to the processing demand from the

control section 105.
[0376]In the medium judgment part 109 which is not illustrated, it is judged whether the storage with which data storage / the playback equipment 101 concerned are loaded is the portability type storage 100 currently recorded by the technique by this invention, or it is the other storage.

[0377]The hash operation part 601 calculates a hash value using a hash function from data.
[0378]Namely, the data recording/playback equipment by this 12th example, In the data recording/playback equipment by a 1st embodiment that was mentioned above, Record the code produced by performing predetermined code extracting processing to data in the processing which records data on said portability type recording medium 100 on a system management area, and. When reading data from said portability type recording medium 100, it is characterized by comparing the code produced by performing said predetermined code extracting processing with said code currently recorded on said system management area.
[0379]And the data recording/playback equipment by the 1st thru/or the 11th example mentioned above are possible also for using together with them suitably, although the data recording/playback equipment by this 12th example are independently.
[0380]Usually, the method of the electronic title used for alteration detection by communication etc. is as follows.
[0381]Creation of an electronic signature: Take out a hash value (generally in an electronic signature, called a message digest) from data using a hash function, encipher it with a secret key, and save as an electronic signature.
using a hash function from the data verified : verified -- a hash value -- taking out (H1) -- an electronic signature is decrypted by a public key, digest data are taken out (H2), and H1 and H2 are compared.
[0382]However, in the case of the data recording/playback equipment by this 12th example, the alteration of data is detectable by an easy technique rather than based on the method of such an electronic title.
[0383]That is, a hash value is calculated using a hash function from data, and he matches it with a data file and is trying to record it on a system management area in the technique by this 12th example.
[0384]It is because a data management area is enciphered, so the user cannot change the hash value of a system management area.
[0385]Therefore, in the technique by this 12th example, even if a user rewrites data, since it is contradictory to the hash value of the data currently recorded on the system management area, an alteration is detectable.
[0386]Drawing 34 is the figure showing the entry composition in FAT16 of the file system by the technique by this 12th example that used the above-mentioned alteration detecting method.
[0387]In this example, it comes to be below the FAT link of one data.
[0388]First, access is started for a FAT entry (ID) from 14 as a start cluster (ID), A FAT entry (ID) shifts to 15 in FH=15, a FAT entry (ID) shifts to 16 in 10H=16, a FAT entry (ID) shifts to 17 in 11H=17, and a FAT entry (ID) shifts to 18 in 12H=18.
[0389]In FFFFH of 18, a FAT entry (ID) is a cluster of the last of a file.
[0390]And the hash value is recorded on the place whose FAT entries (ID) are 19 and 20.
[0391]Drawing 35 is the figure showing the entry composition in the case of the file system applied to the technique by the 6th example that mentioned above the technique by this 12th example that used the above-mentioned alteration detecting method.
[0392]This FAT entry (ID) composition has the number of start cluster ID, the last cluster ID, a hash value, and a defective cluster, ID of the defective cluster 1, ID of the defective cluster 2, etc., as shown in drawing 35.
[0393]Drawing 36 is a key map on portability type recording media, such as a disk explaining the technique by this 12th example that used the above-mentioned alteration detection ****.
[0394]Namely, in the technique by this 12th example. A hash value is calculated using a hash function from data, and he matches the hash value with a data file, and is trying to record it on a system management area in the field in which the data of file file.text of the user area on the

portability type storage 100 is recorded.
[0395]Drawing 37 is a flow chart at the time of the data writing by this 12th example.
[0396]First, as shown in drawing 37, if data is inputted, this process flow will calculate a hash value using a hash function from data, and will record that hash value into FAT (Step S101, S102).
[0397]Next, data is recorded on a portability type storage (Step S103).
[0398]Next, it ends, after updating the information on FAT and a directory entry, and enciphering the data for system managements and recording data on a portability type storage (Step S104, S105, S106).
[0399]drawing 38 is based on this 12th example -- data ****** is carried out and it is a flow chart at the time.
[0400]As shown in drawing 38, this process flow will read and decrypt the data for system managements first, if a file name is inputted (Step S31, S32).
[0401]Next, the information on FAT and a directory entry is acquired, and data is read from a portability type storage (Step S33, S34).
[0402]Next, a hash value is calculated using a hash function from data, and it compares with the hash value currently recorded into the data for system managements (Step S35).
[0403]Next, it judges whether the hash value is in agreement, and it ends, after notifying the thing which are done as it is and for which data is altered if the hash value is not in agreement although it ends, if the hash value is in agreement (Step S36, S37, S38).
[0404]
[Effect of the Invention]Therefore, as explained above, when it stores the mass data of a picture etc. in a portability type storage according to this invention, The data recording/playback equipment which can prevent the alteration which secured the privacy of a data content and bona fides, and includes unjust elimination and destruction of data, and can realize high-speed processing can be provided.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－228060
（P2000－228060A）
(43)公開日　平成12年８月15日(2000.8.15)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ	20/10	Ｈ
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｂ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｄ
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ	9/00	６２１Ｚ
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ	5/91	Ｐ

審査請求　未請求　請求項の数18　ＯＬ　（全 32 頁）　最終頁に続く

(21)出願番号　特願平11－144928

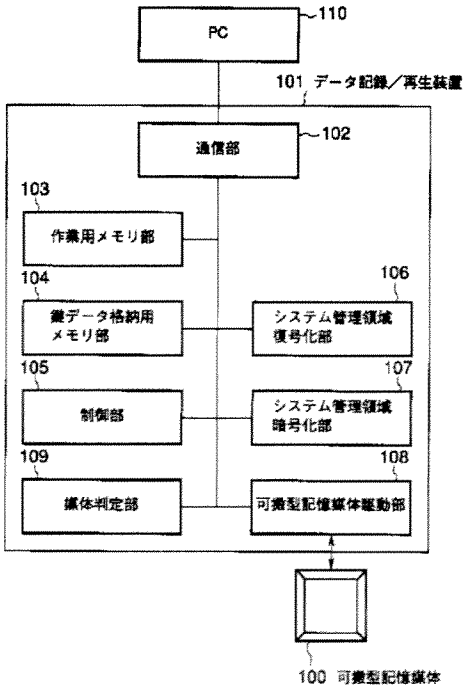
(22)出願日　平成11年５月25日(1999.5.25)

(31)優先権主張番号　特願平10－343013
(32)優先日　平成10年12月２日(1998.12.2)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000000376
オリンパス光学工業株式会社
東京都渋谷区幡ヶ谷２丁目43番２号
(72)発明者　近藤　隆
東京都渋谷区幡ヶ谷２丁目43番２号　オリンパス光学工業株式会社内
(74)代理人　100058479
弁理士　鈴江　武彦　（外４名）

(54)【発明の名称】　可搬型記憶媒体を用いたデータ記録／再生装置

(57)【要約】
【課題】本発明は、大容量の画像データ等を可搬型記憶媒体に格納する際、データ内容の秘匿性、真正性を確保し、且つデータの不正な消去・破壊を含めた改竄を防止でき、且つ高速な処理を実現できるデータ記録／再生装置を提供する。
【解決手段】本発明の一態様によると、システム管理用データが記録されるシステム管理領域及びユーザー用データが記録されるユーザー領域を有する可搬型記憶媒体にデータを記録するデータ記録装置において、暗号化鍵信号又は暗号化鍵信号を生成するための暗号化鍵信号生成情報を含む暗号化秘密情報を保持する暗号化秘密情報保持手段と、前記暗号化秘密情報保持手段に保持されている前記秘密情報暗号化を用いて暗号化処理を行う暗号化手段と、前記暗号化手段により、前記可搬型記憶媒体のシステム管理領域に記録すべきシステム管理用データの少なくとも一部を暗号化処理して前記可搬型記憶媒体のシステム管理領域へ記録する記録手段とを有することを特徴とするデータ記録装置が提供される。



1

【特許請求の範囲】

【請求項１】　システム管理用データが記録されるシステム管理領域及びユーザー用データが記録されるユーザー領域を有する可搬型記憶媒体にデータを記録するデータ記録装置において、

暗号化鍵信号又は暗号化鍵信号を生成するための暗号化鍵信号生成情報を含む暗号化秘密情報を保持する暗号化秘密情報保持手段と、

前記暗号化秘密情報保持手段に保持されている前記暗号化秘密情報を用いて暗号化処理を行う暗号化手段と、

前記暗号化手段により、前記可搬型記憶媒体のシステム管理領域に記録すべきシステム管理用データの少なくとも一部を暗号化処理して前記可搬型記憶媒体のシステム管理領域へ記録する記録手段と、

を有することを特徴とするデータ記録装置。

【請求項２】　前記暗号化手段は、前記可搬型記憶媒体のユーザー領域へユーザー用データの書き込む処理を行っているときに、時間的に、並行して前記可搬型記憶媒体のシステム管理領域に記録すべきシステム管理用データの少なくとも一部の前記暗号化処理を行うことを特徴とする請求項１記載のデータ記録装置。

【請求項３】　システム管理用データが記録されるシステム管理領域及びユーザー用データが記録されるユーザー領域を有する可搬型記憶媒体からデータを読み出すデータ再生装置において、

復号化鍵信号又は復号化鍵信号を生成するための復号化鍵信号生成情報を含む復号化秘密情報を保持する復号化秘密情報保持手段と、

前記復号化秘密情報保持手段に保持されている前記復号化秘密情報を用いて復号化処理を行う復号化手段と、

前記復号化手段により、前記可搬型記憶媒体のシステム管理領域にシステム管理用データの少なくとも一部が前記暗号化秘密情報を用いて暗号化して記録されている前記可搬型記憶媒体のシステム管理領域から前記暗号化されて記録されている前記システム管理用データを読み出し、前記復号化手段を用いて前記暗号化して記録されているシステム管理用データの少なくとも一部を復号するシステム管理用データ再生手段と、

を有することを特徴とするデータ再生装置。

【請求項４】　前記記録手段は、

前記可搬型記録媒体にユーザー用データを記録する際に、このユーザー用データを可搬型記録媒体上で論理的にアクセス可能な単位領域のサイズに分割するデータ分割手段と、

前記可搬型記録媒体のユーザー領域から未使用の単位記録領域を選択する記録領域選択手段と、

前記記録領域選択手段によって選択された複数の未使用の単位記録領域の内の隣接する各領域に対して、前記分割手段によって分割されたデータが不規則な配置で記録されるように、分割されたデータの記録を制御する記録制御手段と、

を有することを特徴とする請求項１記載のデータ記録装置。

2

【請求項５】　前記記録手段は、

前記可搬型記録媒体を初期化する処理の際に、前記可搬型記録媒体の複数の単位記録領域の内、少なくとも１つの単位領域を欠陥領域として前記システム管理用データに登録する欠陥領域登録手段、

を有することを特徴とする請求項１記載のデータ記録装置。

【請求項６】　前記記録手段は、

任意性のあるパラメータを用いてランダムなデータを生成するランダムデータ生成手段と、

前記可搬型記録媒体を初期化する際に、前記ランダムデータ生成手段によって得られたランダムデータを前記可搬型記録媒体のユーザー領域全体に書き込むランダムデータ書き込み手段と、

前記パラメータを前記可搬型記録媒体のシステム管理領域に記録するパラメータ記録手段と、

を有することを特徴とする請求項１記載のデータ記録装置。

【請求項７】　前記ランダムデータ書き込み手段は、

前記可搬型記録媒体からデータを削除する際に、前記可搬型記録媒体のデータ削除領域に前記ランダムデータを再度書き込むものであることを特徴とする請求項６記載のデータ記録装置。

【請求項８】　前記記録手段は、

任意性のあるパラメータを用いてランダムなデータを生成するランダムデータ生成手段と、

前記可搬型記録媒体のユーザー領域から未使用の領域を複数選択する未使用領域選択手段と、

前記未使用領域選択手段により得られた領域に前記ランダムなデータを書き込むランダムデータ書込手段と、

を有することを特徴とする請求項１記載のデータ記録装置。

【請求項９】　前記記録手段は、

前記ユーザー用データを前記ユーザー領域の連続する単位記録領域に従つて連続して記録するものであり、

前記連続する単位記録領域の内、先頭及び最後尾の単位記録領域ＩＤと、前記単位記録領域内の欠陥領域ＩＤとを、前記システム管理領域のファイル管理用テーブルに記録するＩＤ記録手段と、

前記ファイル管理用テーブルに記録されたＩＤに基づき、前記可搬型記録媒体上に記録された前記ユーザー用データの物理的なアドレスを求めるアドレス手段と、

を有することを特徴とする請求項１記載のデータ記録装置。

【請求項１０】　前記記録手段は、

前記ユーザー用データの少なくとも一部に対して、所定の処理を施す処理手段と、

前記処理手段により所定の処理が施された領域のデータ上のアドレス、該アドレスに関連する情報、及び前記所定の処理に必要なパラメータの内の少なくとも一つを前記システム管理用データに記録する処理情報記録手段と、
を有することを特徴とする請求項９記載のデータ記録装置。
【請求項１１】　前記処理手段は、
各単位記録領域内のデータ単位でシャッフルを行うことを特徴とする請求項１０記載のデータ記録装置。
【請求項１２】　前記処理手段は、
各単位記録領域単位でシャッフルを行うことを特徴とする請求項１０記載のデータ記録装置。
【請求項１３】　前記処理手段は、
前記ユーザー用データの全体に対するシヤッフルを行うことを特徴とする請求項１０記載のデータ記録装置。
【請求項１４】　前記処理手段は、
データを暗号化する処理を行うことを特徴とする請求項１０記載のデータ記録装置。
【請求項１５】　前記処理手段は、
単位領域内シヤッフル、単位記録領域単位シヤッフル、前記ユーザー用データの全体に対するシャッフル、及びデータ暗号化の処理の内から少なくとも二つの処理を組み合わせて行うことを特徴とする請求項１０記載のデータ記録装置。
【請求項１６】　前記記録手段は、
前記可搬型記録媒体に記録されるユーザー用データから抽出して得られる所定のコードを前記システム管理領域に記録するコード抽出記録手段、
を有することを特徴とする請求項１記載のデータ記録装置。
【請求項１７】　前記ユーザー用データ再生手段は、
前記可搬型記録媒体から読み出した前記ユーザー用データから所定のコードを抽出するコード抽出手段と、
このコード抽出手段により抽出されたコードと、前記可搬型記録媒体に前記ユーザー用データを記録する際に抽出され前記システム管理領域に予め記録されている前記コードとを前記照合するコード照合手段と、
を有することを特徴とする請求項３記載のデータ再生装置。
【請求項１８】　前記ユーザー用データ再生手段は、
前記システム管理領域から前記パラメータを読み出すパラメータ読み出し手段と、
前記システム管理領域から読み出したパラメータを用いて生成したランダムデータと、前記可搬型記録媒体の未使用領域のクラスタに記載されているランダムデータとを照合する手段と、
を有することを特徴とする請求項３記載のデータ再生装置。
【発明の詳細な説明】

【０００１】
【発明の属する技術分野】本発明は、例えば、光磁気ディスク（ＭＯ）等の可搬型記憶媒体にデータを暗号化して記録すると共に、暗号化して記録されたデータを再生するデータ記録／再生装置及びデータを暗号化して可搬型記憶媒体に記録する際に予め可搬型記憶媒体への不正なアタックに対する防御対策を伴って記録／再生するようにしたデータ記録／再生装置に関する。
【０００２】
【従来の技術】周知のように、デジタル画像等のコンテンツに対し、その内容の秘匿性、真正性（改竄されていないこと）を確保するための技術は、従来から幾つか提案されている。
【０００３】例えば、特公平７－１２２９６０号公報には、デジタルカメラ内に乱数発生装置を設け、デジタルカメラで撮影された画像に対し、デジタルカメラ内で前記乱数系を用いて画像データを暗号化することにより、画像内容の秘匿性や真正性を確保するという手法が開示されている。
【０００４】また、特開平９－２００７３０号公報には、カメラ内で画像データの電子署名を作成することにより、画像データが改竄されているかどうかを検知することができる手法が開示されている。
【０００５】また、光磁気ディスクを用いた医療画像の電子保存システムであるＩＳ＆Ｃ（Ｉｍａｇｅ　Ｓａｖｅ　＆　Ｃａｒｒｙ）システム（参考資料「画像の電子保管とＩＳ＆Ｃシステム」、新医療１９９４年７月号Ｐ３６－４０）では、光磁気ディスクのファイルシステムやデバイスドライバを特殊化すると共に、専用のソフトウェア（データの改変が不可）以外ではアクセスできないようにすることにより、デジタル画像等のコンテンツの秘匿性、真正性を確保している。
【０００６】
【発明が解決しようとする課題】しかしながら、前者の特公平７－１２２９６０号公報や特開平９－２００７３０号公報による手法では、画像内容の漏洩という脅威からコンテンツを保護することは可能であるが、悪意あるユーザーが汎用の計算機等を用いて画像ファイルにアクセスして画像ファイルを消去したり、データ内容を破壊する脅威、すなわち広い意味での画像内容の改竄から、コンテンツを守ることはできない。
【０００７】また、デジタルカメラで撮影される画像は１００万画素を越える大きさであり、このような大きなサイズの画像データを暗号化したり、画像データから電子署名を求めたりする演算量は非常に大きくなり、処理時間も長くなってしまう。
【０００８】特に、デジタルカメラの内部で暗号等の処理を行おうとすると、内部のＣＰＵの処理能力はそれほど大きなものが期待できないため、処理時間は無視できないほど長くなってしまう。

5

【０００９】この問題は、デジタルカメラに連写機能を備える場合などに顕著になる。

【００１０】また、デジタルビデオカメラ装置のように、動画のデータとなると、さらにデータサイズが大きくなるため、処理時間の問題はさらに深刻になる。

【００１１】一方、後者のＩＳ＆Ｃシステムのような専用のファイルシステムでは、データ暗号化の処理を必要としないので処理時間は問題にならない。

【００１２】しかし、ファイルシステムの構造が漏洩してしまった場合には、ある程度保存装置等の知識のあるユーザーなら、可搬型記憶媒体上のファイルにアクセスできてしまう。

【００１３】また、暗号化の手法を使った場合のように、可搬型記憶媒体上のファイルの安全性を守るための情報が漏洩した場合に、暗号化の鍵だけを取りかえれば済むというようなことはできない。

【００１４】さらには、データ内容の安全性確保のための装置としては、むしろ安全性確保のための機構を公開した上でも安全性を確保できることが望ましい。

【００１５】本発明はこれらの点に着目し、画像等の大容量のデータを可搬型記憶媒体に格納する場合に、データ内容の秘匿性、真正性を確保し、且つデータの不正な消去・破壊を含めた改竄を防止でき、且つ高速な処理を実現できるデータ記録／再生装置を提供することを目的とする。

【００１６】

【課題を解決するための手段】本発明によると、上記課題を解決するために、（１）　システム管理用データが記録されるシステム管理領域及びユーザー用データが記録されるユーザー領域を有する可搬型記憶媒体にデータを記録するデータ記録装置において、暗号化鍵信号又は暗号化鍵信号を生成するための暗号化鍵信号生成情報を含む暗号化秘密情報を保持する暗号化秘密情報保持手段と、前記暗号化秘密情報保持手段に保持されている前記暗号化秘密情報を用いて暗号化処理を行う暗号化手段と、前記暗号化手段により、前記可搬型記憶媒体のシステム管理領域に記録すべきシステム管理用データの少なくとも一部を暗号化処理して前記可搬型記憶媒体のシステム管理領域へ記録する記録手段と、を有することを特徴とするデータ記録装置が提供される。

【００１７】また、本発明によると、上記課題を解決するために、（２）　前記前記暗号化手段は、前記可搬型記憶媒体のユーザー領域へユーザー用データの書き込む処理を行っているときに、時間的に、並行して前記可搬型記憶媒体のシステム管理領域に記録すべきシステム管理用データの少なくとも一部の前記暗号化処理を行うことを特徴とする（１）記載のデータ記録装置が提供される。

【００１８】また、本発明によると、上記課題を解決するために、（３）　システム管理用データが記録される

6

システム管理領域及びユーザー用データが記録されるユーザー領域を有する可搬型記憶媒体からデータを読み出すデータ再生装置において、復号化鍵信号又は復号化鍵信号を生成するための復号化鍵信号生成情報を含む復号化秘密情報を保持する復号化秘密情報保持手段と、前記復号化秘密情報保持手段に保持されている前記復号化秘密情報を用いて復号化処理を行う復号化手段と、前記復号化手段により、前記可搬型記憶媒体のシステム管理領域にシステム管理用データの少なくとも一部が前記暗号化秘密情報を用いて暗号化して記録されている前記可搬型記憶媒体のシステム管理領域から前記暗号化されて記録されている前記システム管理用データを読み出し、前記復号化手段を用いて前記暗号化して記録されているシステム管理用データの少なくとも一部を復号するシステム管理用再生手段と、を有することを特徴とするデータ再生装置が提供される。

【００１９】（作用効果）上記（１）又は（３）の発明では、予めデータ記録装置内に暗号化又は復号化を行うための暗号化鍵又は復号化鍵（秘密鍵方式の暗号アルゴリズムを用いる場合は、暗号化鍵と復号化鍵は同じ）、もしくは暗号化鍵や復号化鍵を生成するための秘密情報を格納しておき、可搬型記憶媒体にデータを記録する場合に、可搬型記憶媒体上のシステム管理領域に記録されているルートデイレクトリテーブルのエントリーデータや可搬型記憶媒体上の物理的アドレスと論理的アドレスを対応づける情報が格納されたデータを前記暗号化鍵で暗号化して記録する。

【００２０】このようにすることにより、汎用のデータ記録／再生装置で前記可搬型記憶媒体にアクセスしようとしても、汎用の装置ではデータファイルにアクセスするための情報を読み出すことができないため、データにアクセスできない。

【００２１】また、ユーザーがデータ保存装置に対する知識が深く、例えば、ＳＣＳＩ（Ｓｍａｌｌ　Ｃｏｍｐｕｔｅｒ　Ｓｙｓｔｅｍ　Ｉｎｔｅｒｆａｃｅ）などの低レベルなコマンドを使って、上記データファイルにアクセスするための情報を読み出しても、暗号化の鍵を知らない限り、アクセスするための情報を解読することは極めて困難なため、データにアクセスすることは実際上できない。

【００２２】さらに、本発明による手法では、暗号化するのは可搬型記憶媒体のシステム管理領域に記録されているデータであり、例えば、システム管理用域のデータ全体を暗号化するとしても、このデータのサイズは、画像データや動画像データに比べるとはるかに小さいため、暗号化の演算を施すための処理時間は少なくて済むことになる。

【００２３】例えば、１３０万画素の画像データを圧縮せずにファイルに保存すると、約４メガバイトのデータサイズになるが、一方で１ギガバイトのディスクでも、

システム管理領域のデータサイズは高々数百キロバイトである。

【００２４】つまり、システム管理領域のデータを暗号化するのに比べ、画像データを暗号化しようとすると、上記の例では数百倍の演算量を必要とすることになる。

【００２５】データサイズが数百メガバイト～数ギガバイトにもなる動画データになると、この差はさらに顕著になる。

【００２６】また、上記（２）の発明では、画像等のデータを可搬型記憶媒体中に書き込んでいる時間に並行してシステム管理用データの暗号化処理を行うことにより、暗号化の処理時間によるストレスを解消する。

【００２７】通常、可搬型記憶媒体へデータを書き込む処理には専用のプロセッサが用いられ、そのため暗号化の処理を行うためのプロセッサ（例えば、ＣＰＵ）とは異なる。

【００２８】また、画像データ等の可搬型記憶媒体への書き込みとシステム管理領域のデータを暗号化する処理を並列に行ってもデータ的な問題は起こらない。

【００２９】画像や動画像のデータは数メガバイト～数百メガバイトに達し、データ書き込みにある程度時間を必要とする。

【００３０】したがって、データ書き込み時にシステム管理領域のデータを暗号化する処理を並行に行うことにより、暗号化による処理時間のストレスをなくすことが可能となる。

【００３１】なお、上記（１）乃至（３）の発明は後述する第１の実施の形態が対応し、関連する図は図１乃至図１０である。

【００３２】また、本発明によると、上記課題を解決するために、（４）　前記記録手段は、前記可搬型記録媒体にユーザー用データを記録する際に、このユーザー用データを可搬型記録媒体上で論理的にアクセス可能な単位領域のサイズに分割するデータ分割手段と、前記可搬型記録媒体のユーザー領域から未使用の他に記録領域を選択する記録領域選択手段と、前記記録領域選択手段によって選択された複数の未使用の単位記録領域の内の隣接する各領域に対して、前記分割手段によって分割されたデータが不規則な配置で記録されるように、分割されたデータの記録を制御する記録制御手段と、を有することを特徴とする（１）記載のデータ記録装置が提供される。

【００３３】この（４）の発明は後述する第２の実施の形態が対応し、関連する図は図１２及び図１５乃至図１７である。

【００３４】そして、この（４）の発明中の論理的にアクセス可能な単位領域とは、ＦＡＴファイルシステムなどで言うところのクラスタ領域に対応する。

【００３５】図１５は、データが記録されるときに、ＩＤ＝３，１２，１４，１９に対応するハッチングされた領域で示すデータをクラスタのサイズで分解し、それを連続しないクラスタに記録する概念図を示している。

【００３６】従って、この場合、ＩＤ＝２，４，１３，１８に対応する白抜き領域で示すデータはクラスタのサイズで分解されないものとしている。

【００３７】（作用効果）通常のファイルシステムでは、データを記録する場合、ユーザー領域内で物理的にほぼ連続した領域へ記録する。

【００３８】したがって、上記（１）乃至（３）の発明だけでは、ユーザー領域に直接アクセスしてユーザー領域に記録されているビットパターンを解析することで、記録されているデータの内容が不正に読み出されてしまうという恐れがある。

【００３９】これに対し、この（４）の発明では、データを記録する場合には、まず、データを複数に分割し、その後、分割された各データ同士が物理的に不連続になるようにユーザー領域に記録する。

【００４０】したがつて、ユーザー領域へ直接アクセスして記録されているビットパターンを読み出しても、そこから元のデータを復元することは困難である。

【００４１】例として、可搬型記録媒体として、総容量１ギガバイト、クラスタサイズ１６キロバイトのディスクに、６メガバイト（２００万画素非圧縮の画像データに相当）のデータを記録する場合を考える。

【００４２】この場合、ディスク全体のクラスタ総数は６２５００個であり、また、６メガバイトのファイルを構成するクラスタ数は３７５個であるので、可能なデータの順序付の組み合わせ数Ｃは、データサイズが既知の場合でも、

$$C = 65200! / (65200-375)!$$

であるから、Ｃは、ほぼ65200^{375}　通りも存在し、総当たり的に元のデータを解読することは実際上不可能である。

【００４３】また、本発明によると、上記課題を解決するために、（５）　前記記録手段は、前記可搬型記録媒体を初期化する処理の際に、前記可搬型記録媒体の複数の単位記録領域の内、少なくとも一つの単位領域を欠陥領域として前記システム管理用データに登録する欠陥領域登録手段、を有することを特徴とする（１）記載のデータ記録装置が提供される。

【００４４】この（５）の発明は後述する第２の実施の形態が対応し、関連する図は図１８及び図１９である。

【００４５】（作用効果）この（５）の発明によれば、ユーザー領域内にデータを記録できない欠陥領域を複数配置する（ＦＡＴファイルシステムの場合では、ＦＡＴエントリの一部に欠陥クラスタであることを示すコードを記録する）ことで、データを記録する際に記録媒体上での連続性を低下させ、その結果、ユーザー領域に直接アクセスしてユーザー領域に記録されているビットパターンを解析することでデータが不正に読み出されてしま

うという危険性を下げることができる。

【００４６】また、この（５）の発明では、媒体初期化時に欠陥領域を記録する以外は、上記（１）乃至（３）の発明の処理と同じであるという構造の単純さと、処理が軽いというメリットがある。

【００４７】また、本発明によると、上記課題を解決するために、（６）　前記記録手段は、任意性のあるパラメータを用いてランダムなデータを生成するランダムデータ生成手段と、前記可搬型記録媒体を初期化する際に、前記ランダムデータ生成手段によって得られたランダムデータを前記可搬型記録媒体のユーザー領域全体に書き込むランダムデータ書き込み手段と、前記パラメータを前記可搬型記録媒体のシステム管理領域に記録するパラメータ記録手段と、を有することを特徴とする（１）記載のデータ記録装置が提供される。

【００４８】また、本発明によると、上記課題を解決するために、（７）　前記ランダムデータ書き込み手段は、前記可搬型記録媒体からデータを削除する際に、前記可搬型記録媒体のデータ削除領域に前記ランダムデータを再度書き込むものであることを特徴とする（６）記載のデータ記録装置が提供される。

【００４９】この（６）及び（７）の発明は後述する第２の実施の形態が対応し、関連する図は図２０乃至図２２である。

【００５０】（作用効果）通常、可搬型記録媒体の初期化（出荷）時には、ユーザー領域は均一の値（各ビットがが全てＯＮ、あるいはすべてＯＦＦ）となっている。

【００５１】したがって、可搬型記録媒体上に少数のデータしか記録されていない場合には、上記（４）の発明で述べたような総当たり的アタックに対して組み合わせの数が少なくなるためデータの安全性の度合いが低くなる。

【００５２】しかるに、この（６）及び（７）の発明によると、可搬型記録媒体のユーザー領域は、可搬型記録媒体の初期化時にランダムな値が記録されているため、媒体上に少数のデータしか記録されていない場合でも、記録されていない領域のビットのＯＮ／ＯＦＦが一様でないため、アタックするためには総当たり的な手法が必要になり、データの安全性が向上する。

【００５３】また、本発明によると、上記課題を解決するために、（８）　前記記録手段は、任意性のあるパラメータを用いてランダムなデータを生成するランダムデータ生成手段と、前記可搬型記録媒体のユーザー領域から未使用の領域を複数選択する未使用領域選択手段と、前記未使用領域選択手段により得られた領域に前記ランダムなデータを書き込むランダムデータ書込手段と、を有することを特徴とする（１）記載のデータ記録装置が提供される。

【００５４】この（８）の発明は後述する第２の実施の形態が対応し、関連する図は図２０及び図２３である。

【００５５】（作用効果）可搬型記録媒体のユーザー領域にデータを書き込む前からデータを改竄することを意図するならば、データを書き込む前のユーザー領域のビットパターンを全部ダンプして記録しておき、書き込んだ後に再びユーザー領域のビットパターンをすべてダンプし、両方のビットパターンを比較して差分をとると、書き込んだデータが記録されている領域の特定ができてしまう。

【００５６】したがって、可搬型記録媒体上に少数のデータしか記録されていない場合には、上記（４）の発明で述べたような総当たり的アタックに対して組み合わせの数が少なくなるためデータの安全性の度合いが低くなる。

【００５７】しかるに、この（８）の発明によると、可搬型記録媒体のユーザー領域にデータを書き込むとき、同時にダミーのデータを実際に記録したいデータと共に書き込むことで、上記のアタックに対してデータの安全性が向上する。

【００５８】また、本発明によると、上記課題を解決するために、（９）　前記記録手段は、前記ユーザー用データを前記ユーザー領域の連続する単位記録領域に従つて連続して記録するものであり、前記連続する単位記録領域の内、先頭及び最後尾の単位記録領域ＩＤと、前記単位記録領域内の欠陥領域ＩＤとを、前記システム管理領域のファイル管理用テーブルに記録するＩＤ記録手段と、前記ファイル管理用テーブルに記録されたＩＤに基づき、前記可搬型記録媒体上に記録された前記ユーザー用データの物理的なアドレスを求めるアドレス手段と、を有することを特徴とする（１）記載のデータ記録装置が提供される。

【００５９】この（９）の発明は後述する第２の実施の形態が対応し、関連する図は図２４及び図２５である。

【００６０】（作用効果）例えば、高精細のデジタルカメラ等で撮影されたデータのサイズは一般に大きく、したがって、その撮影データを可搬型記録媒体に記録するときに使用するＦＡＴエントリの個数も大きくなる。

【００６１】前述したように、クラスタサイズ１６キロバイトのディスクへ６メガバイト（２００万画素非圧縮の画像データに相当）のデータを記録する場合、３７５個のＦＡＴエントリが必要になる。

【００６２】そして、ＦＡＴのエントリが大きくなれば、上記（１）乃至（３）の発明における暗号化／復号化処理の負担が大きくなる。

【００６３】一方、データを記録するときに、データが書き込まれる先頭位置と最後尾の位置が分かるような情報をシステム管理領域に記録することでもデータにアクセスすることは可能である。

【００６４】この場合、必要なＦＡＴエントリの数は最少２個で済むが、データを記録する領域中に欠陥クラスタがあれば、その位置及び個数を記録しなければならな

いので、その分必要なエントリの数が増えるが、通常ほとんどゼロであるので、１つの画像をユーザー領域に書き込むときに必要なＦＡＴエントリの数は、データが書き込まれる先頭位置と最後尾の位置が分かるような情報、及び書き込む領域内に存在する欠陥クラスタの個数を表す情報の３つである。

【００６５】したがって、前述の６メガバイトのデータを書き込む場合、必要になるＦＡＴエントリの個数は１００分の１以下になる。

【００６６】このことは、データ再生装置の暗号化／復号化の処理速度向上のために、非常に有効な手段となる。

【００６７】また、本発明によると、上記課題を解決するために、（１０）　前記記録手段は、前記ユーザー用データの少なくとも一部に対して、所定の処理を施す処理手段と、前記処理手段により所定の処理が施された領域のデータ上のアドレス、該アドレスに関連する情報、及び前記所定の処理に必要なパラメータの内の少なくとも一つを前記システム管理用データに記録する処理情報記録手段と、を有することを特徴とする（９）記載のデータ記録装置が提供される。

【００６８】この（１０）の発明は後述する第２の実施の形態が対応し、関連する図は図２４乃至図２７である。

【００６９】また、本発明によると、上記課題を解決するために、（１１）　前記処理手段は、各単位記録領域内のデータ単位でシャッフルを行うことを特徴とする（１０）記載のデータ記録装置が提供される。

【００７０】この（１１）の発明は後述する第２の実施の形態が対応し、関連する図は図２４乃至図２８及び図３０である。

【００７１】また、本発明によると、上記課題を解決するために、（１２）　前記処理手段は、各単位記録領域単位でシャッフルを行うことを特徴とする（１０）記載のデータ記録装置が提供される。

【００７２】この（１２）の発明は後述する第２の実施の形態が対応し、関連する図は図２４乃至図２９である。

【００７３】また、本発明によると、上記課題を解決するために、（１３）　前記処理手段は、前記ユーザー用データの全体に対するシヤッフルを行なうことを特徴とする（１０）記載のデータ記録装置が提供される。

【００７４】この（１３）の発明は後述する第２の実施の形態が対応し、関連する図は図２４乃至図２８及び図３１である。

【００７５】また、本発明によると、上記課題を解決するために、（１４）　前記処理手段は、データを暗号化する処理を行うことを特徴とする（１０）記載のデータ記録装置が提供される。

【００７６】この（１４）の発明は後述する第２の実施の形態が対応し、関連する図は図２４乃至図２７及び図３２である。

【００７７】また、本発明によると、上記課題を解決するために、（１５）　前記処理手段は、単位領域内シヤッフル、単位記録領域単位シヤッフル、前記ユーザー用データの全体に対するシャッフル、及びデータ暗号化の処理の内から少なくとも二つの処理を組み合わせて行うことを特徴とする（１０）記載のデータ記録装置が提供される。

【００７８】この（１５）の発明は後述する第２の実施の形態が対応し、関連する図は図２４乃至図２８及び図３０、図３２である。

【００７９】（作用効果）上記（９）の発明では、データをユーザー領域上で連続的に記録することを前提としている。

【００８０】したがって、このままでは、ユーザー領域に直接アクセスしてユーザー領域に記録されているビットパターンを解析することで、そこに記録されているデータの内容を不正に読み出されてしまうという恐れがある。

【００８１】そこで、（１０）の発明では、データを記録するときに、そのまま記録するのではなく、データをシヤッフルしたり暗号化する等の処理を施して記録することをでデータの安全性を高める処理を施す。

【００８２】この際に、シャッフルや暗号化の処理に必要なパラメータを上記（９）の発明のＦＡＴエントリ中に図２６に示すようにして埋め込めば、データ毎にデータを保護するための様々な処理バリエーションを加えることが可能となり、且つ、上記（９）の発明の効果であるＦＡＴのサイズを小さくできるという効果も得ることができる。

【００８３】また、（１１）乃至（１５）の発明は、データの安全性を高めるための処理を行うものである。

【００８４】また、本発明によると、上記課題を解決するために、（１６）　前記記録手段は、前記可搬型記録媒体に記録されるユーザーデータから抽出して得られる所定のコードを前記システム管理領域に記録するコード抽出記録手段、を有することを特徴とする（１）記載のデータ記録装置が提供される。

【００８５】また、本発明によると、上記課題を解決するために、（１７）　前記システム管理用データ再生手段は、前記可搬型記録媒体から読み出した前記ユーザー用データから所定のコードを抽出するコード抽出手段と、このコード抽出手段により抽出されたコードと、前記可搬型記録媒体に前記ユーザー用データを記録する際に抽出され前記システム管理領域に予め記録されている前記コードとを前記照合するコード照合手段と、を有することを特徴とする（３）記載のデータ再生装置が提供される。

【００８６】この（１６）及び（１７）の発明は後述す

る第２の実施の形態が対応し、関連する図は図３４乃至図３８である。

【００８７】（作用効果）上記（１０）乃至（１５）の発明が記録するデータをスクランブルしてデータを読めなくすることでデータの安全性を確保する発明であったのに対し、この（１６）及び（１７）の発明ならびに後述する（１８）の発明はデータを読み出すことは可能だが、改竄すると改竄したことがわかるような仕組みを施すことでデータの安全性を確保する発明である。

【００８８】この場合、基本的な考え方としては、通信等で用いられているメッセージ認証子（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ：ＭＡＣ）の方法に基づいている。

【００８９】以下に、このＭＡＣの方法を説明する。

【００９０】ＭＡＣを用いてデータの改竄を検知する方法では、まず、データに所定の演算（通常、方向性関数であるＨＡＳＨ関数（ハッシュ値）が用いられる）を施してメッセージ・ダイジェスト（ＭＤ）と呼ばれるコードを取り出す。

【００９１】このＭＤは、ＨＡＳＨ関数の性質から元のデータの内容が少しでも変わると大きく変化するという特徴がある。

【００９２】次に、第３者から厳重に秘密を守られた暗号鍵を用いてＭＤを暗号化する。

【００９３】この暗号化されたＭＤがＭＡＣであり、通信時にはデータと共にこのＭＡＣを通信相手に送信する。

【００９４】受信した側では、まず、データから上述と同じようにデータに所定の演算を施してＭＤを得る。

【００９５】次に、一緒に受信したＭＡＣから、復号化の鍵を用いて復号化してＭＤ´を得る。

【００９６】もし、通信途中でデータが改竄されるとＭＤとＭＤ´とは異なるコードになるため、ＭＤとＭＤ´とを比較することで通信途中におけるデータの改竄の有無を調べることができる。

【００９７】以上がＭＡＣによるデータの改竄検知の方法である。

【００９８】因みに、ＭＤを暗号化するときにデータ送信側と受信側で同じ暗号化／復号化鍵を用いる共通鍵暗号方式のアルゴリズムを用いたコードをＭＡＣ、データ送信側が秘密鍵でＭＤを暗号化し、受信側がそれを公開鍵で復号化した場合を一般に電子署名と呼ぶ場合もあるが、この発明では両者を総称してＭＡＣと呼ぶことにする。

【００９９】（１６）の発明では、データを（９）の発明による手法でユーザー領域に記録するときに、まず、ＭＤを求める。

【０１００】その後、このＭＤを図３５に示すように（９）の発明のＦＡＴエントリ中にＭＤ（ハッシュ値）を記録する。

【０１０１】通常、ＭＡＣの場合には、ＭＤを通信等の途中で改竄されないように暗号化する必要がある。

【０１０２】しかし、本発明では前提としてシステム管理領域全体が暗号化されるようになつている。

【０１０３】したがって、ＭＤを、特に、暗号化しないでシステム管理領域にあるＦＡＴエントリに記録してもＭＡＣと同様の効果を得ることができる。

【０１０４】さらには、本発明では、改竄検知の処理をパスするモードを設けることで、上記（３）の発明と同じ処理速度でデータを読み出すことが可能になるという効果が得られる。

【０１０５】（１７）の発明は、上記（１６）の発明によって記録されたＭＤ（ハッシュ値）を用いて改竄検知のための照合処理を行うもので、上記（３）の発明によるデータ再生装置に適用される。

【０１０６】また、本発明によると、上記課題を解決するために、（１８）　前記システム管理用データ再生手段は、前記システム管理領域から前記パラメータを読み出すパラメータ読み出し手段と、前記システム管理領域から読み出したパラメータを用いて生成したランダムデータと、前記可搬型記録媒体の未使用領域のクラスタに記載されているランダムデータとを照合する手段と、を有することを特徴とする（３）記載のデータ再生装置が提供される。

【０１０７】この（１８）の発明は後述する第２の実施の形態が対応し、関連する図は図２０乃至図２２である。

【０１０８】（作用効果）この（１８）の発明は、上記（６），（７）の発明のデータ記録装置で記録されたデータを読み出すためのデータ再生装置である。

【０１０９】この（１８）の発明によれば、悪意あるユーザーが他の記録装置を用いてデータを不正に消去した場合でも、消去されたユーザー領域のビットパターンが上記（６），（７）の発明によつて記録されたパターンと異なることから、不正にデータを消去したという痕跡を残すことができるという効果が得られる。

【０１１０】

【発明の実施の形態】以下図面を参照して本発明の実施の形態について説明する。

【０１１１】（第１の実施形態）まず、図１、図３、図４、図６乃至図１０を用いて、本発明によるデータ記録／再生装置の第１の実施形態について説明する。

【０１１２】なお、これらの各図中で同じ番号が割り当てられた部分は、同じ機能を持つものとする。

【０１１３】図１は、第１の実施形態におけるデータ記憶／再生装置の構成を示すブロック図である。

【０１１４】すなわち、このデータ記憶／再生装置１０１は、外部のＰＣ１１０と通信を行う通信部１０２と、この通信部１０２にそれぞれ内部バスを介して接続されている作業用メモリ部１０３、鍵データ記憶用メモリ部

１０４、制御部１０５、復号化部１０６、暗号化部１０７、可搬型記憶媒体駆動部１０８、媒体判定部１０９から構成される。

【０１１５】通信部１０２は、ＳＣＳＩ（Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ ＳｙｓｔｅｍＩｎｔｅｒｆａｃｅ）やイーサネット、シリアルケーブル等の通信ケーブル、あるいは赤外線などの無線を用いて、データ記録／再生装置外部のＰＣ１１０やワークステーションなどのデータ作成・編集装置とデータやコマンドのやり取りをする機能を持つ。

【０１１６】作業用メモリ１０３は、通信部１０２などから送られてきたデータや、各種処理の途中段階のデータをバッファリングすると共に、プログラムをロードするためのメモリである。

【０１１７】また、鍵データ格納用メモリ部１０４は、秘密情報、例えば、ＤＥＳ等の暗号鍵を格納するためのメモリである。

【０１１８】制御部１０５は、データ記憶／再生装置１０１の処理全体を制御する部分である。

【０１１９】復号化部１０６は、鍵データ格納用メモリ部１０４からデータを復号化するための情報を読み出し、データを復号化する。

【０１２０】同様に暗号化部１０７は、鍵データ格納用メモリ部１０４からデータを暗号化するための情報を読み出し、データを暗号化する。

【０１２１】また、可搬型記憶媒体駆動部１０８は、制御部１０５からの処理要求に応じ、当該データ記憶／再生装置１０１に装填される可搬型記憶媒体１００上の領域のデータの読み出し／書き込み（消去を含む）を行う。

【０１２２】媒体判定部１０９は、当該データ記憶／再生装置１０１に装填される記憶媒体が、本発明による手法で記録されている可搬型記憶媒体１００であるか、それ以外の記憶媒体であるかを判定する。

【０１２３】図３は、一般的なファイルシステムを説明するための図であり、ここではＷｉｎｄｏｗｓやＭＳ－ＤＯＳで用いられているＦＡＴファイルシステムの記憶媒体１上の構成を示している。

【０１２４】一般に、ＦＡＴファイルシステムの記憶媒体１では、システム管理領域７として、ブートセクタ（ＯＥＭ　ＩＤやローダールーチン、デバイスに関する情報が記録されているＢＰＢ、及び予約領域からなる）２、ＦＡＴ３、ＦＡＴのコピー４、及びルートディレクトリのエントリテーブル５で構成されていると共に、ユーザー領域８としてファイル領域６で構成されている（詳細は次の文献を参照：“ＭＳ－ＤＯＳエンサイクロペディアＶｏｌｕｍｅ１”、アスキー出版局（１９８９）ｐ１１２－１１８）。

【０１２５】一方、図４は、本発明による第１の実施形態で用いられる可搬型記憶媒体１００上の構成を示している。

【０１２６】図４では、システム管理領域７のデータは、図１の鍵データ格納用メモリ部１０４に格納されている暗号化鍵データと同じ鍵データで、且つ暗号化部１０７の暗号化法と同じ方法で暗号化されて記録されている。

【０１２７】図６は、本発明による第１の実施形態におけるデータ読み出し時の処理の流れを示すフローチャートである。

【０１２８】可搬型記憶媒体１００からデータを読み出すときには、外部のＰＣ１１０等からの可搬型記憶媒体１００上のデータ読み出し要求（ステップＳ１）に応じて、まず、可搬型記憶媒体１００のシステム管理領域に暗号化されて記録されているシステム管理用データを、可搬型記憶媒体駆動部１０８を用いて作業用メモリ１０３へ読み出す（ステップＳ２）。

【０１２９】その後、読み出した暗号化されているシステム管理用データを、復号化部１０６を用いて復号化し（ステップＳ３）、システム管理用のデータを得る。

【０１３０】システム管理用のデータが得られたならば、その情報を用いて指定のデータを読み出し（ステップＳ４）、通信部１０１を介して外部のＰＣ１１０へ読み出したデータを送信して終了する（ステップＳ５）。

【０１３１】図７は、第１の実施形態で可搬型記憶媒体１００へ初めてアクセスしてデータを読み出すときの処理の流れを示すフローチャートである。

【０１３２】可搬型記憶媒体１００へ初めてアクセスしてデータを読み出すときには、外部のＰＣ１１０等からの可搬型記憶媒体１００上のデータ読み出し要求（ステップＳ２１）に応じて、まず、アクセスが初めてであるか否かを判定（ステップＳ２２）する。

【０１３３】そして、アクセスが初めてあるときには、可搬型記憶媒体１００のシステム管理領域に暗号化されて記録されているシステム管理用データを、可搬型記憶媒体駆動部１０８を用いて作業用メモリ１０３へ読み出す（ステップＳ２３）。

【０１３４】その後、読み出した暗号化されているシステム管理用データを、復号化部１０６を用いて復号化し（ステップＳ２４）、システム管理用のデータを得る。

【０１３５】システム管理用のデータが得られたならば、その情報を用いて指定のデータを読み出し（ステップＳ２５）、通信部１０２を介して外部のＰＣ１１０へ読み出したデータを送信して終了する（ステップＳ２６）。

【０１３６】しかるに、ステップＳ２２において、アクセスが初めてではないときには、上記のステップＳ２３，Ｓ２４の処理をスルーして、前に得られているシステム管理用のデータの情報を用いて指定のデータを読み出し（ステップＳ２５）、通信部１０２を介して外部のＰＣ１１０へ読み出したデータを送信して終了する（ス

テップＳ２６）。

【０１３７】図８は、第１の実施形態でデータを書き込むときの処理の流れを示すフローチャートである。

【０１３８】通信部１０２を介して外部のＰＣ１００から受け取ったデータを可搬型記憶媒体１００へ書き込む場合には、まず、読み出し時と同様の手順で、システム管理用のデータを作業用メモリ１０３へ読み出す（ステップＳ４０、Ｓ４１）。

【０１３９】その後、復号化されたシステム管理用のデータを用いて、外部のＰＣ１００から受け取ったデータを可搬型記憶媒体１００へ書き込む（ステップＳ４２、Ｓ４３）。

【０１４０】このとき、可搬型記憶媒体１００上のデータの構成が更新されているので、当然、作業用メモリ１０３上のシステム管理用のデータも更新する（ステップＳ４４）。

【０１４１】その後、作業用メモリ１０３上のシステム管理用のデータを暗号化部１０７を用いて暗号化し（ステップＳ４５）、可搬型記憶媒体駆動部１０８を用いて上記暗号化したシステム管理用のデータを可搬型記憶媒体１００のシステム管理領域に書き込み（ステップＳ４６）、終了する（ステップＳ４７）。

【０１４２】図９は、第１の実施形態で可搬型記憶媒体１００へ初めてアクセスしてデータを書き込むときの処理の流れを示すフローチャートである。

【０１４３】可搬型記憶媒体１００へ初めてアクセスしてデータを書き込むときには、外部のＰＣ１１０等からの可搬型記憶媒体１００上のデータ書き込み要求（ステップＳ６０）に応じて、まず、アクセスが初めてであるか否かを判定（ステップＳ６１）する。

【０１４４】そして、アクセスが初めてあるときには、可搬型記憶媒体１００のシステム管理領域に暗号化されて記録されているシステム管理用データを、可搬型記憶媒体駆動部１０８を用いて作業用メモリ１０３へ読み出す（ステップＳ６２）。

【０１４５】その後、復号化されたシステム管理用のデータを用いて、外部のＰＣ１００から受け取ったデータを可搬型記憶媒体１００へ書き込む（ステップＳ６３、Ｓ６４）。

【０１４６】このとき、可搬型記憶媒体１００上のデータの構成が更新されているので、当然、作業用メモリ１０３上のシステム管理用のデータも更新する（ステップＳ６５）。

【０１４７】その後、作業用メモリ１０３上のシステム管理用のデータを暗号化部１０７を用いて暗号化し（ステップＳ６６）、可搬型記憶媒体駆動部１０８を用いて上記暗号化したシステム管理用のデータを可搬型記憶媒体１００のシステム管理領域に書き込み（ステップＳ６７）、終了する（ステップＳ６８）。

【０１４８】しかるに、ステップＳ６１において、アクセスが初めてではないときには、上記のステップＳ６２，Ｓ６３の処理をスルーして、前に得られているシステム管理用のデータの情報を用いて、外部のＰＣ１００から受け取ったデータを可搬型記憶媒体１００へ書き込む（ステップＳ６３、Ｓ６４）。

【０１４９】このとき、可搬型記憶媒体１００上のデータの構成が更新されているので、当然、作業用メモリ１０３上のシステム管理用のデータも更新する（ステップＳ６５）。

【０１５０】その後、作業用メモリ１０３上のシステム管理用のデータを暗号化部１０７を用いて暗号化し（ステップＳ６６）、可搬型記憶媒体駆動部１０８を用いて上記暗号化したシステム管理用のデータを可搬型記憶媒体１００のシステム管理領域に書き込み（ステップＳ６７）、終了する（ステップＳ６８）。

【０１５１】すなわち、システム管理用のデータは、毎回暗号化して可搬型記憶媒体１００のシステム管理領域に書き込まれることになる。

【０１５２】図１０の（ａ）は、第１の実施形態で可搬型記憶媒体１００へ初めてアクセスしてデータを書き込むときの処理の流れを示す他のフローチャートである。

【０１５３】可搬型記憶媒体１００へ初めてアクセスしてデータを書き込むときには、外部のＰＣ１１０等からの可搬型記憶媒体１００上のデータ書き込み要求（ステップＳ８０）に応じて、まず、アクセスが初めてであるか否かを判定（ステップＳ８１）する。

【０１５４】そして、アクセスが初めてあるときには、可搬型記憶媒体１００のシステム管理領域に暗号化されて記録されているシステム管理用データを、可搬型記憶媒体駆動部１０８を用いて作業用メモリ１０３へ読み出す（ステップＳ８２）。

【０１５５】その後、復号化されたシステム管理用のデータを用いて、外部のＰＣ１００から受け取ったデータを可搬型記憶媒体１００へ書き込む（ステップＳ８３、Ｓ８４）。

【０１５６】このとき、可搬型記憶媒体１００上のデータの構成が更新されているので、当然、作業用メモリ１０３上のシステム管理用のデータも更新して（ステップＳ８５）、終了する（ステップＳ８６）。

【０１５７】しかるに、ステップＳ８１において、アクセスが初めてではないときには、上記のステップＳ８２，Ｓ８３の処理をスルーして、前に得られているシステム管理用のデータの情報を用いて、外部のＰＣ１００から受け取ったデータを可搬型記憶媒体１００へ書き込む（ステップＳ８４）。

【０１５８】このとき、可搬型記憶媒体１００上のデータの構成が更新されているので、当然、作業用メモリ１０３上のシステム管理用のデータも更新して（ステップＳ８５）、終了する（ステップＳ８６）。

【０１５９】図１０の（ｂ）は、第１の実施形態で可搬

型記憶媒体１００の排出要求があったときの処理の流れを示すフローチャートである。

【０１６０】すなわち、可搬型記憶媒体１００の排出要求があったときには、システム管理用データを暗号化（ステップＳ９１）し、この暗号化されたシステム管理用のデータを可搬型記憶媒体１００上のシステム管理領域に記録（ステップＳ９２）した後、可搬型記憶媒体１００を排出する（ステップＳ９３）。

【０１６１】すなわち、可搬型記憶媒体１００を本発明によるデータ記録／再生装置１０１から排出するときだけ、システム管理用データを暗号化して可搬型記憶媒体１００上のシステム管理領域に記録するものである。

【０１６２】なお、以上の説明では、システム管理領域のデータを全て暗号化しているが、図５に示すように、ＦＡＴ、ＦＡＴのコピー、及びルートディレクトリのエントリテーブルのみを暗号化するようにしてもよい。

【０１６３】また、ここまでの説明ではデータ記録装置の外部装置としてＰＣを例に説明したが、外部の装置としては、これに限定されない。

【０１６４】例えば、ＰＣの代わりにワークステーション、ＰＤＡ等の情報編集機器であってもよいし、あるいはスキャナーやデジタルカメラ、デジタルビデオカメラのような映像撮像装置であっても構わない。

【０１６５】なお、この発明の実施の形態の各構成は、当然、各種の変形、変更が可能である。

【０１６６】図２に示すように、映像撮像装置１３０としては、光学系１２０、撮像部１２１、Ａ／Ｄ変換部１２２、画像処理部１２３、フォーマット変換部１２４、ユーザーインタフエイス部１２５から構成されるとともに、データ記録／再生装置１０１としての構成要素である作業用メモリ部１０３、鍵データ記憶用メモリ部１０４、制御部１０５、復号化部１０６、暗号化部１０７、可搬型記憶媒体駆動部１０８、媒体判定部１０９から構成される。

【０１６７】光学系１２０は、レンズ、鏡筒駆動系などから構成され、映像を撮像部１２１に結像する。

【０１６８】また、撮像部１２１は光信号を電気信号に変換し、Ａ／Ｄ変換部１２２では、前記電気信号をＡ／Ｄ変換してデジタル化したデータを作業用メモリ部１０３へ格納する。

【０１６９】画像処理部１２３では、前記の作業用メモリ１０３に格納されたデジタルデータから、画像を生成するための各種処理（例えば、ホワイトバランスの調整、ガンマ変換、エッヂ強調処理など）を施す。

【０１７０】フォーマット変換部１２４は、前記の画像のデータをＪＰＥＧ等の保存形式に変換する部分である。

【０１７１】また、ユーザーインタフェイス部１２５は、シャッター、液晶ファインダー、各種撮影モード設定用のボタンなどのユーザーインタフェイスからなる。

【０１７２】ファイルの消去などの要求もユーザーインタフェイス部１２５を介して入力される。

【０１７３】図２から分かるように、上記のような構成でも、図２の点線内は第１の実施形態のデータ記録／再生装置と同じである。

【０１７４】また、第１の実施形態の場合に、通信部１０２を通して外部のＰＣ１１０等とデータのやり取りをしていた部分が、図２では映像撮像装置内の点線外部との間でデータをやり取りすることに置き換わっただけである。

【０１７５】したがって、図２のような構成においても、第１の実施形態の機能を備えることが可能である。

【０１７６】上記のような構成によって、画像のような大容量のデータを、データ内容の秘匿性、真正性を確保し、且つ高速にデータを記録できるデータ記録装置を提供することが可能になる。

【０１７７】そして、上述したような第１の実施の形態には、以下のような発明が含まれている。

【０１７８】（１）　可搬型記憶媒体にデータを記録するデータ記録／再生装置において、装置内に秘密情報を保持する手段と、前記秘密情報を用いて暗号化及び復号化を行う手段と、前記暗号化手段を用いて、前記可搬型媒体のシステム管理用データ、もしくはシステム管理用データの一部を暗号化して前記可搬型記憶媒体のシステム管理領域へ記録する手段と、前記可搬型記憶媒体のシステム管理領域から、前記暗号化された前記システム管理用データを読み出し、前記復号化手段を用いて前記暗号化されたシステム管理用データ、もしくは暗号化されたシステム管理用データの一部を復号化する手段と、を有することを特徴とするデータ記録／再生装置。

【０１７９】（２）　前記データ記録／再生装置は、データを前記可搬型記憶媒体のユーザー領域へ書き込む処理を行っているときに、時間的に並行して前記暗号化の処理を行うことを特徴とするデータ記録／再生装置。

【０１８０】（第２の実施形態）ところで、上述したような第１の実施形態による手法においては、可搬型記録媒体上のデータをダンプして、順次読み出し位置を変えるという不正なアタック方法でデータ内容を読み出される可能性を有しているという危険がある。

【０１８１】特に、デジタルカメラで撮影した画像を格納するような記録媒体の場合、撮影するデータの種類（“ＷＯＲＤ”，“ｅｘｃｅｌ”，“ｔｅｘｔ”，“ｊｐｅｇ”“ｔｉｆｆ”，“ｍｐｅｇ”等のフォーマットのこと）も決まっており（ＪＰＥＧ，ＴＩＦＦ，ＦｌａｓｈＰｉｘ等）、さらにデータサイズもＣＣＤの画素数が固定であることによってほぼ一定であるので、第１の実施形態による手法においては、上述のような不正なアタックに対して弱いという難点がある。

【０１８２】そこで、この第２の実施形態では、このような不正なアタックに対する防御対策を伴ったデータ記

録／再生装置を提供することを意図している。

【０１８３】まず、この第２の実施形態で用いる用語について説明する。

【０１８４】

（１）論理的にアクセス可能な単位領域＝クラスタ

（２）物理的にアクセス可能な単位領域＝セクタ

（３）ＦＡＴ　　：Ｆｉｌｅ　Ａｌｌｏｃａｔｉｏｎ　Ｔａｂｌｅの略語であり、ＭＳ－ＤＯＳのファイルシステム名である。以下の説明の中では、ＦＡＴをファイルシステムが用いる管理テーブルの総称のように用いているが、“ＦＡＴ”というのは飽くまでＭＳ－ＤＯＳやＷｉｎｄｏｗｓで用いられているファイルシステムで用いている管理テーブルの名称である。

（４）疑似欠陥クラスタ：実際に物理的に壊れているわけではなく、正常か欠陥かを示す管理テーブルの内容を操作することで欠陥としたクラスタ（本明細書内での定義）。

（５）疑似ランダム　　：疑似乱数系列を用いて乱数を生成するため、“疑似”という言葉が付く。

【０１８５】次に、第２の実施形態の概要について説明する。

【０１８６】この第２の実施形態では、システム管理領域（ＦＡＴを含む）を暗号化することをベースに、大きく分けて以下の５つの手法が含まれている。

【０１８７】（１）データに対するクラスタの物理的な配置を疑似ランダム化する（連続性をなくす）。

【０１８８】（２）疑似欠陥クラスタを作り、データの読み出しを困難にする。

【０１８９】なお、上記（１），（２）に従属して以下のケースがある。

【０１９０】ａ）データ初期化時に、ユーザー領域を疑似ランダムデータで初期化する。

【０１９１】ｂ）データ削除のときは、その領域を元のランダムデータに置き換える。

【０１９２】これは、未使用かつ初期化時と異なるデータが記録されたクラスタがあるときに改竄の疑いありとするためである。

【０１９３】（３）データ書き込み時にＭＯディスク等の記録媒体の未使用領域（上記疑似欠陥クラスタ領域も含む）に偽のデータも同時に書き込む。

【０１９４】なお、この（３）はについては、上記（１）、（２）と併用可能である。

【０１９５】（４）データに対する追記がない、データのサイズがほぼ一定であることを利用し、ＦＡＴの小規模化（ＦＡＴ暗号化の演算量を削減）を実現する。

【０１９６】なお、この（４）に従属して以下のケースがある。

【０１９７】ａ）データ記録時にシャッフルするなどの各種処理を行う。

【０１９８】ｂ）処理のパラメータをシステム管理領域に記録する。

【０１９９】（５）データ記録時に、データのハッシュ値（ＯＲ　Ｅｒｒｏｒ　Ｃｏｒｒｅｃｔｉｎｇ　Ｃｏｄｅ／Ｅｒｒｏｒ　Ｄｅｔｅｃｔｉｎｇ　Ｃｏｄｅ）を求め、システム管理領域に記録する。

【０２００】図１１は、以上のような概要に基づく第２の実施形態の上記の５つの手法に対応するＭＳ－ＤＯＳ　ＦＡＴ１６ファイルシステムのファイル管理手法を説明するための図である。

【０２０１】すなわち、図１１は、ファイル名ｆｉｌｅ．ｔｅｘｔのファイルに対するアクセスを例にとったものである。

【０２０２】この場合、ルートディレクトリのエントリ（又は、サブディレクトリのエントリ）を検索することにより、図１１中にメニュー形式で示すようなｆｉｌｅ．ｔｅｘｔのディレクトリエントリ（ＦＡＴ１６）を探す。

【０２０３】ここでは、開始クラスタ（ＩＤ）としてＦＡＴエントリ（ＩＤ）が１４である場合を示している。

【０２０４】なお、図１１中にメニュー形式で示すようなファイルの大きさは、４８００ｂｙｔｅｓであって、例えば、１クラスタ＝１０２４ｂｙｔｅｓであれば、５クラスタが必要となる場合を示している。

【０２０５】また、ここでは、１クラスタ＝２セクタ＝１０２４ｂｙｔｅｓである場合を示している。

【０２０６】図１１中の“Ｈ”は、１６進数を意味するものとする。

【０２０７】そして、ＦＡＴエントリ（ＩＤ）が１１，１２，１３，１４，１５，１６，１７，１８，１９，２０に対して、各クラスタＣＨ，ＤＨ，ＦＦＦＦＨ，ＦＨ，１０Ｈ，１２Ｈ，ＦＦＦ７Ｈ，１３Ｈ，ＦＦＦＦＨ，０Ｈがそれぞれ上記疑似ランダムによるランダム化されて割り当てられている例である。

【０２０８】この例では、１つのデータのＦＡＴリンク以下のようになる。

【０２０９】まず、開始クラスタ（ＩＤ）としてＦＡＴエントリ（ＩＤ）が１４からアクセスが開始され、ＦＨ＝１５でＦＡＴエントリ（ＩＤ）が１５に移行し、１０Ｈ＝１６でＦＡＴエントリ（ＩＤ）が１６に移行し、１２Ｈ＝１８でＦＡＴエントリ（ＩＤ）が１８に移行し、１３Ｈ＝１９でＦＡＴエントリ（ＩＤ）が１９に移行する。

【０２１０】なお、ＦＡＴエントリ（ＩＤ）が１７のＦＦＦ７Ｈは、上記疑似欠陥クラスタ領域としての不良クラスタであるため、ＦＡＴエントリ（ＩＤ）が１６からＦＡＴエントリ（ＩＤ）が１８に移行している。

【０２１１】また、ＦＡＴエントリ（ＩＤ）が１９のＦＦＦ８～ＦＦＦＦＨは、ファイルの最後のクラスタである。

【０２１２】そして、ＦＡＴエントリ（ＩＤ）が２０の

０Ｈは、未使用クラスタである。

【０２１３】次に、以上のような概要に基づく第２の実施形態の上記の５つの手法に対応する各具体例について図１２乃至図３７を参照して説明する。

【０２１４】なお、これらの各図中で上述した第１の実施形態と同じ番号が割り当てられた部分は、同じ機能を持つものとする。

【０２１５】（第１の具体例）まず、図１２乃至図１７を用いて、本発明によるデータ記録／再生装置の第２の実施形態の第１の具体例について説明する。

【０２１６】図１２は、第２の実施形態における第１の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【０２１７】すなわち、このデータ記憶／再生装置１０１は、外部のＰＣ１１０と通信を行う通信部１０２と、この通信部１０２にそれぞれ内部バスを介して接続されている作業用メモリ部１０３、鍵データ記憶用メモリ部１０４、制御部１０５、復号化部１０６、暗号化部１０７、可搬型記憶媒体駆動部１０８、媒体判定部１０９（図示せず、第１の実施形態参照）、データ分割部２０１、クラスタ選択部２０２から構成される。

【０２１８】通信部１０２は、ＳＣＳＩ（Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ ＳｙｓｔｅｍＩｎｔｅｒｆａｃｅ）やイーサネット、シリアルケーブル等の通信ケーブル、あるいは赤外線などの無線を用いて、データ記録／再生装置外部のＰＣ１１０やワークステーションなどのデータ作成・編集装置とデータやコマンドのやり取りをする機能を持つ。

【０２１９】作業用メモリ１０３は、通信部１０２などから送られてきたデータや、各種処理の途中段階のデータをバッファリングすると共に、プログラムをロードするためのメモリである。

【０２２０】また、鍵データ格納用メモリ部１０４は、秘密情報、例えば、ＤＥＳ等の暗号鍵を格納するためのメモリである。

【０２２１】制御部１０５は、データ記憶／再生装置１０１の処理全体を制御する部分である。

【０２２２】復号化部１０６は、鍵データ格納用メモリ部１０４からデータを復号化するための情報を読み出し、データを復号化する。

【０２２３】同様に暗号化部１０７は、鍵データ格納用メモリ部１０４からデータを暗号化するための情報を読み出し、データを暗号化する。

【０２２４】また、可搬型記憶媒体駆動部１０８は、制御部１０５からの処理要求に応じ、当該データ記憶／再生装置１０１に装填される可搬型記憶媒体１００上の領域のデータの読み出し／書き込み（消去を含む）を行う。

【０２２５】なお、図示しない媒体判定部１０９では、当該データ記憶／再生装置１０１に装填される記憶媒体が、本発明による手法で記録されている可搬型記憶媒体１００であるか、それ以外の記憶媒体であるかを判定する。

【０２２６】データ分割部２０１は、データを可搬型記録媒体１００上で論理的にアクセス可能な単位領域のサイズに分割する。

【０２２７】クラスタ選択部２０２は、所定の規則に従って可搬型記録媒体１００から使用されていないクラスタを論理的にアクセス可能な単位領域のクラスタとして選択する。

【０２２８】すなわち、この第１の具体例によるデータ記録／再生装置は、上述したような第１の実施形態によるデータ記録／再生装置において、データを可搬型記録媒体１００に記録する処理において、データ分割部２０１によりデータを可搬型記録媒体１００上で論理的にアクセス可能な単位領域のサイズに分割すると共に、クラスタ選択部２０２により所定の規則に従って可搬型記録媒体１００から使用されていないクラスタを論理的にアクセス可能な単位領域のクラスタとして選択することにより、制御部１０５からの処理要求に応じて前記分割されたデータを前記選択された論理的にアクセス可能な単位領域のクラスタに逐次記録することを特徴としている。

【０２２９】すなわち、通常、データを可搬型記録媒体としての例えばＭＯ等のディスクに記録するときには、クラスタが連続的につながっている領域にデータを記録するようにしているが、この方法だと、ディスクのユーザー領域を順次ダンプしていくことで、ディスクに書き込まれたデータが読み出されるという脅威がある。

【０２３０】そこで、この第１の具体例によるデータ記録／再生装置では、データを書き込むときに、あえて連続性のないクラスタを選んでデータを書き込むことで、上記脅威を回避する手法を採用するものとしている。

【０２３１】例えば、ディスクサイズ１Ｇ、画像サイズ６Ｍ（２００万画素非圧縮）の場合、クラスタのサイズが１６Ｋのケースでも、ディスク全体のクラスタ数は６２５００個あり、画像データ１つを記録するためのクラスタ数は３７５個ある。

【０２３２】このようなディスクに対して第１の具体例による手法を採用すれば、システム管理領域が暗号化されてクラスタ間のリンクが分からない場合には、手探りで画像データを復元しようにも、６２５００個のクラスタから（初期化時にディス．クの全領域にランダムなデータを書き込んでいるので）正しい順番で３７５個のクラスタに記録されたデータを読みださなければならず、解読は相当困難になる（単純計算で約62500^{375}　通りの組み合わせがある）。

【０２３３】仮に、データを書き込む前と後の記録媒体全領域がダンプされ、前記２つのダンプされたデータ比較することにより、データが記録されている領域があば

かれたとしても、データを読み出すためのデータの順番がわからないので、３７５！通りの組み合わせから本当のデータを解読する必要がある。

【０２３４】実際には、画像データの場合、周波数や色相関などの情報から、３７５！通りよりもう少し探索範囲を狭めることは可能ではあるが、解読自体は不可能に近いと言える。

【０２３５】そして、この第１の具体例による手法では、クラスタの物理的な連続性がなくなるため、読み出し速度は低下するが、基本的に通常のファイルステムと同じで、システム管理領域のデータサイズは変わらない。

【０２３６】図１３は、この第１の具体例による手法に基づいたＦＡＴ１６ファイルシステムにおけるデータ管理形態を示している。

【０２３７】すなわち、図１３は、先に第２の実施形態の概要について説明した図１１からクラスタ部分を取り出して示したものであって、疑似欠陥クラスタ領域を設けていない以外は図１１に準じている。

【０２３８】この例では、１つのデータのＦＡＴリンク以下のようになる。

【０２３９】まず、開始クラスタ（ＩＤ）としてＦＡＴエントリ（ＩＤ）が１４からアクセスが開始され、ＦＨ＝１５でＦＡＴエントリ（ＩＤ）が１５に移行し、１０Ｈ＝１６でＦＡＴエントリ（ＩＤ）が１６に移行し、１１Ｈ＝１７でＦＡＴエントリ（ＩＤ）が１７に移行し、１２Ｈ＝１８でＦＡＴエントリ（ＩＤ）が１８に移行する。

【０２４０】なお、ＦＡＴエントリ（ＩＤ）が１８のＦＦＦＨは、ファイルの最後のクラスタである。

【０２４１】図１４は、通常のファイルシステムを用いた場合に、システム管理領域とユーザー領域とを有する可搬型記録媒体のユーザー領域にデータが記録されるときの例を参考的に示している。

【０２４２】この場合、可搬型記録媒体では、データの物理的配置として、例えば、ＩＤ（アドレス）＝２～３７のクラスタ領域をできるだけ物理的な連続性を確保するように配置されている。

【０２４３】そして、この図１４においては、ハッチングを有するＩＤ（アドレス）＝１４～１８のクラスタ領域にデータが書き込まれる例を示している。

【０２４４】図１５は、この第１の具体例による手法に基づいたデータの記録形態を示している。

【０２４５】すなわち、この図１５においては、記録するデータは、まず、クラスタのサイズに分割され、各々、ランダムに選択されたクラスタＩＤ（アドレス）＝２，３，４…１２，１３，１４…１７，１８，１９…３３のクラスタ領域に記録されることを示している。

【０２４６】図１６は、この第１の具体例による場合の１つのデータのＦＡＴリンクを図１４の一部と対応付けて示している。

【０２４７】この図１６から分かるように、基本的にＦＡＴシステムで扱うことが可能な手法である。

【０２４８】図１７は、この第１の具体例によるファイルシステムを用いた場合に、システム管理領域とユーザー領域とを有する可搬型記録媒体のユーザー領域にデータが記録されるときの例を示している。

【０２４９】この場合、可搬型記録媒体では、データの物理的配置として、例えば、ＩＤ（アドレス）＝２～３７のクラスタ領域をできるだけ物理的な連続性をなくすようにランダム化して配置されている。

【０２５０】そして、この図１７においては、ハッチングを有するＩＤ（アドレス）＝３，１２，１４，１７，１９，３３クラスタ領域にデータが書き込まれる例を示している。

【０２５１】（第２の具体例）次に、図１８及び図１９を用いて、本発明によるデータ記録／再生装置の第２の実施形態の第２の具体例について説明する。

【０２５２】図１８は、第２の実施形態における第２の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【０２５３】すなわち、このデータ記憶／再生装置１０１は、外部のＰＣ１１０と通信を行う通信部１０２と、この通信部１０２にそれぞれ内部バスを介して接続されている作業用メモリ部１０３、鍵データ記憶用メモリ部１０４、制御部１０５、復号化部１０６、暗号化部１０７、可搬型記憶媒体駆動部１０８、媒体判定部１０９（図示せず、第１の実施形態参照）、クラスタ選択部３０１、乱数発生部３０２から構成される。

【０２５４】通信部１０２は、ＳＣＳＩ（Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ ＳｙｓｔｅｍＩｎｔｅｒｆａｃｅ）やイーサネット、シリアルケーブル等の通信ケーブル、あるいは赤外線などの無線を用いて、データ記録／再生装置外部のＰＣ１１０やワークステーションなどのデータ作成・編集装置とデータやコマンドのやり取りをする機能を持つ。

【０２５５】作業用メモリ１０３は、通信部１０２などから送られてきたデータや、各種処理の途中段階のデータをバッファリングすると共に、プログラムをロードするためのメモリである。

【０２５６】また、鍵データ格納用メモリ部１０４は、秘密情報、例えば、ＤＥＳ等の暗号鍵を格納するためのメモリである。

【０２５７】制御部１０５は、データ記憶／再生装置１０１の処理全体を制御する部分であり、後述する欠陥クラスタ情報の書き込み制御はこの制御部１０５で行われることになる。

【０２５８】復号化部１０６は、鍵データ格納用メモリ部１０４からデータを復号化するための情報を読み出し、データを復号化する。

【０２５９】同様に暗号化部１０７は、鍵データ格納用メモリ部１０４からデータを暗号化するための情報を読み出し、データを暗号化する。

【０２６０】また、可搬型記憶媒体駆動部１０８は、制御部１０５からの処理要求に応じ、当該データ記憶／再生装置１０１に装填される可搬型記憶媒体１００上の領域のデータの読み出し／書き込み（消去を含む）を行う。

【０２６１】なお、図示しない媒体判定部１０９では、当該データ記憶／再生装置１０１に装填される記憶媒体が、本発明による手法で記録されている可搬型記憶媒体１００であるか、それ以外の記憶媒体であるかを判定する。

【０２６２】クラスタ選択部３０１は、所定の規則に従って可搬型記録媒体１００から論理的にアクセス可能な単位領域のクラスタとして選択する。

【０２６３】乱数発生部３０２は、後述する欠陥クラスタ情報の書き込み制御に用いられるランダムなデータとして任意性のあるパラメータを用いたランダムデータを生成するための乱数を発生する。

【０２６４】すなわち、この第２の具体例によるデータ記録／再生装置は、上述したような第１の実施形態によるデータ記録／再生装置において、データを可搬型記録媒体１００に記録する処理において、クラスタ選択部３０１及び乱数発生部３０２とにより前記可搬型記録媒体１００から論理的にアクセス可能な単位領域をランダムに複数選ぶと共に、制御部１０５により前記可搬型記録媒体１００上で論理的にアクセス可能な単位領域を欠陥領域として前記システム管理用データに登録することを特徴としている。

【０２６５】そして、この第２の具体例では、初期化時に、可搬型記録媒体１００上にランダムに疑似欠陥クラスタを作ることを特徴としている。

【０２６６】ここでいう疑似欠陥クラスタとは、実際にユーザー領域のクラスタを破壊するのではなく、単に、ＦＡＴエントリに対応するクラスタが壊れているという情報を記録するだけである（システム管理用データを暗号化しているので、この情報は誰にも分からない）。

【０２６７】記録媒体に書き込まれるデータは、真のデータの所々に疑似欠陥セクタが入り込んでいる。

【０２６８】例えば、全クラスタの１０％が疑似欠陥セクタの場合、前例の条件では（３７５＋３８）個のクラスタに３８個の疑似欠陥クラスタ（偽データ）が含まれていることになる。

【０２６９】従って、データを読み出すためには６２５００個のクラスタ全体から、データが記録されている領域を探し出し、その後、さらに疑似欠陥クラスタの部分を取り除く必要がある。

【０２７０】仮に、データを書き込む前と後の記録媒体全領域がダンプされ、前記２つのダンプされたデータ比較することにより、データが記録されている領域があばかれたとしても、後述する第６乃至第１１の具体例による手法と併用することにより、データ内容を強靭に保護することが可能である。

【０２７１】なお、ＪＰＥＧ等の圧縮画像の場合には、各クラスタに記録されているデータそのものが直接画像を表現しないため、第６乃至第１１の具体例による手法と併用することは特に必要なく、この第２の具体例による手法のみでデータ内容を強靭に保護することが可能である。

【０２７２】この第２の具体例による手法では、疑似欠陥クラスタの分だけディスク領域に無駄が生じることになる。

【０２７３】しかし、この第２の具体例の場合、欠陥クラスタ情報は通常の方法で図１１に示したようにＦＡＴエントリ内に記録されるため、わざわざ欠陥クラスタ情報（位置）をＦＡＴ以外のところに別途記録しておく必要はない。

【０２７４】そして、この第２の具体例による手法では、基本的に通常のファイルステムと同じであるため実装が簡単であると共に、データを書き込むクラスタに連続性があるためデータの書き込み速度が速いという利点がある。

【０２７５】図１９の（ａ），（ｂ）は、通常の場合のＦＡＴリンクの初期化状態と、この第２の具体例による手法に基づいたＦＡＴリンクの初期化状態とを対比させて示している。

【０２７６】すなわち、図１９の（ａ）に示すように、通常の場合のＦＡＴリンクの初期化状態では、通常の場合と何等変わりがない。

【０２７７】これに対し、図１９の（ｂ）に示すように、この第２の具体例による手法では、ＦＡＴエントリ（ＩＤ）＝１２，１７のところに、ＦＦＦ７Ｈなる疑似欠陥クラスタ領域であることを示すコードが付されている。

【０２７８】（第３の具体例）次に、図２０乃至図２２を用いて、本発明によるデータ記録／再生装置の第２の実施形態の第３の具体例について説明する。

【０２７９】図２０は、第２の実施形態における第３の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【０２８０】すなわち、このデータ記憶／再生装置１０１は、外部のＰＣ１１０と通信を行う通信部１０２と、この通信部１０２にそれぞれ内部バスを介して接続されている作業用メモリ部１０３、鍵データ記憶用メモリ部１０４、制御部１０５、復号化部１０６、暗号化部１０７、可搬型記憶媒体駆動部１０８、媒体判定部１０９（図示せず、第１の実施形態参照）、クラスタ照合部４０１、乱数発生部４０２から構成される。

【０２８１】通信部１０２は、ＳＣＳＩ（Ｓｍａｌｌ

Ｃｏｍｐｕｔｅｒ　ＳｙｓｔｅｍＩｎｔｅｒｆａｃｅ）やイーサネット、シリアルケーブル等の通信ケーブル、あるいは赤外線などの無線を用いて、データ記録／再生装置外部のＰＣ１１０やワークステーションなどのデータ作成・編集装置とデータやコマンドのやり取りをする機能を持つ。

【０２８２】作業用メモリ１０３は、通信部１０２などから送られてきたデータや、各種処理の途中段階のデータをバッファリングすると共に、プログラムをロードするためのメモリである。

【０２８３】また、鍵データ格納用メモリ部１０４は、秘密情報、例えば、ＤＥＳ等の暗号鍵を格納するためのメモリである。

【０２８４】制御部１０５は、データ記憶／再生装置１０１の処理全体を制御する部分である。

【０２８５】復号化部１０６は、鍵データ格納用メモリ部１０４からデータを復号化するための情報を読み出し、データを復号化する。

【０２８６】同様に暗号化部１０７は、鍵データ格納用メモリ部１０４からデータを暗号化するための情報を読み出し、データを暗号化する。

【０２８７】また、可搬型記憶媒体駆動部１０８は、制御部１０５からの処理要求に応じ、当該データ記憶／再生装置１０１に装填される可搬型記憶媒体１００上の領域のデータの読み出し／書き込み（消去を含む）を行う。

【０２８８】なお、図示しない媒体判定部１０９では、当該データ記憶／再生装置１０１に装填される記憶媒体が、本発明による手法で記録されている可搬型記憶媒体１００であるか、それ以外の記憶媒体であるかを判定する。

【０２８９】クラスタ照合部４０１は、後述するように、システム管理領域から読み出したパラメータを用いて生成したランダムデータと、前記可搬型記録媒体の未使用領域のクラスタに記録されているデータとが初期化時と同じであるか否かを照合する。

【０２９０】乱数発生部４０２は、後述するユーザー領域全体に前記ランダムデータの書き込み制御に用いられるランダムなデータとして任意性のあるパラメータを用いたランダムデータを生成するための乱数を発生する。

【０２９１】すなわち、この第３の具体例によるデータ記録／再生装置は、上述したような第１の実施形態によるデータ記録／再生装置において、データを可搬型記録媒体１００に記録する処理において、前記可搬型記録媒体を初期化するために、乱数発生部４０２により任意性のあるパラメータを用いてランダムなデータを生成して、制御部１０５からの処理要求に応じてユーザー領域全体に前記ランダムデータを書き込むと共に、前記システム管理領域に予め記録しておいた前記パラメータを読み出し、クラスタ照合部４０１により前記システム管理領域から読み出したパラメータを用いて生成したランダムデータと、前記可搬型記録媒体の未使用領域のクラスタに記録されているデータとが初期化時と同じであるか否かを照合し、制御部１０５からの処理要求に応じて前記可搬型記録媒体からデータを削除するときに、前記可搬型記録媒体の未使用の領域に疑似ランダムデータを書き込むことを特徴としている。

【０２９２】そして、この第３の具体例による手法は、前述した第１及び第２の具体例による手法を補うものである。

【０２９３】すなわち、通常、データを可搬型記録媒体としての例えばＭＯ等のディスクに記録するときに、データが記録されていないディスクはディスク領域全体が例えば０（ＯＦＦ）で初期化されている場合が考えられる。

【０２９４】そのような場合、前述した第１及び第２の具体例による手法だけではデータが記録されている領域とされていない領域は、ディスク全体をダンプすることですぐに分かってしまうという脅威がある。

【０２９５】そこで、この第３の具体例による手法では、予めデイスク全体をランダムな値で初期化してしまうことにより、上記脅威を低減させる手法である。

【０２９６】この手法は、データを記録した後でデータ内容を改竄するアタックに対しては効果がある。

【０２９７】しかるに、この第３の具体例による手法では、データ記録前と記録後の差分をとるというアタックには何ら効果がないが、このアタックに対する対策は次に述べる第４の具体例による手法で対策することができる。

【０２９８】また、ファイルシステムに関する知識を有し、かつ悪意あるユーザーによって上記の初期化されたディスクのユーザー領域が他のデータ記録装置で低レベルの手段を用いて０などに一様に初期化される恐れがある。

【０２９９】そこで、この第３の具体例による手法では、未使用の領域には場所に依存する特定のデータ（疑似ランダムデータ）を書き込み、ユーザー領域に不正にデータが書き込まれていないかをチェックすることができる機能を備える。

【０３００】このため、第３の具体例による手法では、具体的には、疑似乱数生成系列とその種（ここでは、パラメータと呼び、シスアム管理領域に暗号化して記録されるもの）を用いる。

【０３０１】すなわち、乱数生成の種が分かっていれば、どのクラスタにどんな乱数列が記録されたか分かるため、上記のようにユーザー領域に不正にデータが書き込まれていないかをチェックすることができるからである。

【０３０２】また、通常、データファイルを消去する場合には、単に、ＦＡＴエントリから対応するＦＡＴリン

ク部分を未使用（０Ｈ）にするだけであるが、このようにすると上記の手法を採用することができない。

【０３０３】そこで、この第３の具体例による手法では、消去した場合には、そのファイルが使用していたクラスタの値を、上記乱数の種を用いて、初期化時と同じ値にするようにしている。

【０３０４】図２１は、この第３の具体例による手法を説明するための概念図である。

【０３０５】図２２は、この第３の具体例による手法を説明するためのフローチャートである。

【０３０６】すなわち、ＦＡＴエントリのＩＤをｎとし、システム管理領域に予め記録しておく前記パラメータをｘとするとき、これらのｎ，ｘをランダムデータ生成装置に入力して１クラスタ分のランダムデータを生成する（ステップＳ１１，Ｓ１２，Ｓ１３）。

【０３０７】そして、この１クラスタ分のランダムデータを可搬型記録媒体のユーザー領域におけるｎ番目のクラスタに記録するようにすることにより、ユーザー領域をランダムな値で全面的に初期化すると共に、システム管理用データを暗号化して可搬型記録媒体のシステム管理領域に記録した後、終了する（ステップＳ１４，Ｓ１５，Ｓ１６，Ｓ１７）。

【０３０８】（第４の具体例）次に、図２３を用いて、本発明によるデータ記録／再生装置の第２の実施形態の第４の具体例について説明する。

【０３０９】図２３は、第２の実施形態における第４の具体例によるデータ記録／再生装置の機能を説明するためのフローチャートである。

【０３１０】なお、この第４の具体例によるデータ記録／再生装置の構成については、前述した第３の具体例によるデータ記録／再生装置の構成と同じであるため、その説明を省略するものとする。

【０３１１】すなわち、この第４の具体例によるデータ記録／再生装置は、上述したような第１の実施形態によるデータ記録／再生装置において、データを可搬型記録媒体１００に記録する処理において、乱数発生部４０２により任意性のあるパラメータを用いてランダムなデータを生成して、制御部１０５からの処理要求に応じてユーザー領域から複数選択した未使用の領域に前記ランダムなデータを書き込むことを特徴としている。

【０３１２】そして、この第４の具体例は、図２３に示すように、ディスクにデータを記録するとき（ステップＳ５１，Ｓ５２）に、ダミーデータを同時に記録する（ステップＳ５３～Ｓ５７）という手法である。

【０３１３】すなわち、ダミーデータの同時記録については、ＦＡＴエントリのＩＤをｎとするとき、このｎをランダムデータ生成装置に入力してランダムデータを生成する（ステップＳ５３，Ｓ５４）。

【０３１４】そして、未使用のクラスタ領域をランダムに選択し、この選択したクラスタ領域にランダムデータをＮ≦ｎ（但し、Ｎは、ランダムデータを書き込むクラスタ領域数）となるまで記録するようにすると共に、システム管理用データを暗号化して可搬型記録媒体のシステム管理領域に記録した後、終了する（ステップＳ５５，Ｓ５６，Ｓ５７，Ｓ５８，Ｓ５９）。

【０３１５】この第４の具体例による手法では、システム管理データが第１の実施形態に示したように暗号化されているので、ダミーデータが真のデータと一緒に記録されていることについては、ユーザーからは見分けがつかない。

【０３１６】また、ダミーデータは未使用領域（疑似欠陥クラスタを含む）を未使用のステータスのままで使うので、ディスク等の可搬型記録媒体領域をまったく無駄にしない（ＦＡＴには一切記録しないので、ファイルにならない）。

【０３１７】（第５の具体例）次に、図２４及び図２５を用いて、本発明によるデータ記録／再生装置の第２の実施形態の第５の具体例について説明する。

【０３１８】図２４は、第２の実施形態における第５の具体例によるデータ記録／再生装置の機能を説明するためにＦＡＴエントリ構成を示している図である。

【０３１９】このＦＡＴエントリ（ＩＤ）構成は、図２４に示すように、開始クラスタＩＤ、最後のクラスタＩＤ、欠陥クラスタの個数、欠陥クラスタ１のＩＤ、欠陥クラスタ２のＩＤ等を有している。

【０３２０】図２５の（ａ），（ｂ）は、第１の具体例に準じた場合のＦＡＴファイルシステムと、この第５の具体例による手法に基づいたファイルシステムとを対比させて示している図である。

【０３２１】すなわち、図２５の（ａ）に示すように、第１の具体例に準じた場合のＦＡＴファイルシステムでは、第１の具体例の場合とほぼ変わりがない。

【０３２２】これに対し、図２５の（ｂ）に示すように、この第２の具体例による手法では、ＦＡＴエントリ（ＩＤ）＝Ｋ－１，Ｋ，Ｋ＋１，Ｋ＋２，Ｋ＋３，Ｋ＋４，Ｋ＋５において、開始クラスタ（ＩＤ）としてＦＡＴエントリ（ＩＤ）がＫ（１４）からアクセスが開始され、Ｋ＋１（１５），Ｋ＋２（１），Ｋ＋３（１７）に移行する。

【０３２３】なお、この第５の具体例によるデータ記録／再生装置の構成については、前述した第２の具体例によるデータ記録／再生装置の構成と同じであるため、その説明を省略するものとする。

【０３２４】すなわち、この第５の具体例によるデータ記録／再生装置は、上述したような第１の実施形態によるデータ記録／再生装置において、データを可搬型記録媒体１００に記録する処理において、前記システム管理領域に、データを記録する領域の、論理的にアクセス可能な先頭及び最後尾の単位領域のＩＤと、前記データを記録する連続領域内の欠陥領域の情報をファイル管理用

テーブルに記録すると共に、前記可搬型記録媒体上のデータに対する読み出し、書き込み等のアクセスを行う場合に、前記ファイル管理用テーブルからデータの可搬型記録媒体上の物理的なアドレスを求めることを特徴としている。

【０３２５】そして、この第５の具体例による手法は、以下に示すような観点に基づいている。

【０３２６】例えば、デジタルカメラのデータ記録装置の場合、２００万画素の非圧縮データならば、そのデータのサイズは６Ｍバイトであり、ＦＡＴ１６のシステムでは必要なクラスタ数は、クラスタサイズを１６Ｋバイトとしても３６７個となり、１つの画像ファイルを管理するのに必要な管理データは３６７×２＝７３４バイト必要になる。

【０３２７】ところで、デジタルカメラでは、通常データに対して後から追記するような処理は行われないと共に、１つのデータは通常連続するクラスタに連続して記録される。

【０３２８】従って、通常のＦＡＴシステムの場合のようにＦＡＴの全てをリンクする必要はなく、クラスタの開始ＩＤ（アドレス）と最後のＩＤ及び、途中に欠陥クラスタがある場合にはその情報が記録されていれば、データにアクセスすることが可能である。

【０３２９】最近のＭＯ等のディスクでは、欠陥クラスタがほとんど存在しないのが普通であるため、上記の手法でデータファイルを管理するのに必要な領域は、上記の例の場合、ＦＡＴ１６システムの数百分の１になる。

【０３３０】本システムでは、システム管理領域を暗号化することを考えると、システム管理領域のデータ量の削減は処理時間の短縮には極めて有効な手段であると考えられる。

【０３３１】この第５の具体例による手法は、連続するクラスタを用いることが条件であるため、上述した第１、第３及び第４の具体例による手法に対しては適用することができない。

【０３３２】（第６乃至第１１の具体例）次に、図２６乃至及び図３２を用いて、本発明によるデータ記録／再生装置の第２の実施形態の第６乃至第１１の具体例について説明する。

【０３３３】なお、この第６乃至第１１の具体例は、いずれも前述した第５の具体例による手法に従属的に適用されるものである。

【０３３４】すなわち、この第６乃至第１１の具体例は、前述した第５の具体例による手法が、データファイルを管理するのに必要なファイルシステムのデータ量を少なくできることを利用し、ファイルシステムのデータに書き込むデータをファイルに異なるでシャッフルしたり、暗号化したりできるようにする手法である。

【０３３５】図２６は、第２の実施形態における第６乃至第１１の具体例によるデータ記録／再生装置の機能を共通に説明するためにＦＡＴエントリ構成を示している図である。

【０３３６】このＦＡＴエントリ（ＩＤ）構成は、図２６に示すように、開始クラスタＩＤ、最後のクラスタＩＤ、処理情報、欠陥クラスタの個数、欠陥クラスタ１のＩＤ、欠陥クラスタ２のＩＤ等を有している。

【０３３７】図２７は、第２の実施形態における第６乃至第１１の具体例によるデータ記録／再生装置の機能を共通に説明するためのフローチャートである。

【０３３８】この処理フローは、図２７に示すように、まず、データが入力されると、データ処理情報を作成してＦＡＴ中に記録する（ステップＳ７１，Ｓ７２）。

【０３３９】次に、データ処理情報に従って入力データを処理すると共に、可搬型記憶媒体上にデータを記録する（ステップＳ７３，Ｓ７４）。

【０３４０】次に、ＦＡＴ及びディレクトリエントリの情報を更新すると共に、システム管理用データを暗号化して可搬型記憶媒体上にデータを記録した後、終了する（ステップＳ７５，Ｓ７６，Ｓ７７）。

【０３４１】そして、第６の具体例によるデータ記録／再生装置は、上述したような第５の具体例によるデータ記録／再生装置において、データを前記可搬型記憶媒体のユーザー領域へ書き込む処理を行うときに、データ全体、もしくはデータの一部に対して所定の処理を施すと共に、前記処理を施した領域のデータ上のアドレス、またはアドレスに関連する情報、及び前記処理に必要なパラメータをシステム管理用データに記録することを特徴としている。

【０３４２】図２８は、第２の実施形態における第７の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【０３４３】すなわち、このデータ記憶／再生装置１０１は、外部のＰＣ１１０と通信を行う通信部１０２と、この通信部１０２にそれぞれ内部バスを介して接続されている作業用メモリ部１０３、鍵データ記憶用メモリ部１０４、制御部１０５、復号化部１０６、暗号化部１０７、可搬型記憶媒体駆動部１０８、媒体判定部１０９（図示せず、第１の実施形態参照）、シャッフル処理部５０１から構成されている。

【０３４４】通信部１０２は、ＳＣＳＩ（Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ ＳｙｓｔｅｍＩｎｔｅｒｆａｃｅ）やイーサネット、シリアルケーブル等の通信ケーブル、あるいは赤外線などの無線を用いて、データ記録／再生装置外部のＰＣ１１０やワークステーションなどのデータ作成・編集装置とデータやコマンドのやり取りをする機能を持つ。

【０３４５】作業用メモリ１０３は、通信部１０２などから送られてきたデータや、各種処理の途中段階のデータをバッファリングすると共に、プログラムをロードするためのメモリである。

【０３４６】また、鍵データ格納用メモリ部１０４は、秘密情報、例えば、ＤＥＳ等の暗号鍵を格納するためのメモリである。

【０３４７】制御部１０５は、データ記憶／再生装置１０１の処理全体を制御する部分である。

【０３４８】復号化部１０６は、鍵データ格納用メモリ部１０４からデータを復号化するための情報を読み出し、データを復号化する。

【０３４９】同様に暗号化部１０７は、鍵データ格納用メモリ部１０４からデータを暗号化するための情報を読み出し、データを暗号化する。

【０３５０】また、可搬型記憶媒体駆動部１０８は、制御部１０５からの処理要求に応じ、当該データ記憶／再生装置１０１に装填される可搬型記憶媒体１００上の領域のデータの読み出し／書き込み（消去を含む）を行う。

【０３５１】なお、図示しない媒体判定部１０９では、当該データ記憶／再生装置１０１に装填される記憶媒体が、本発明による手法で記録されている可搬型記憶媒体１００であるか、それ以外の記憶媒体であるかを判定する。

【０３５２】シャッフル処理部５０１は、上述したような第６の具体例によるデータ記録／再生装置において、前記所定の処理として、ブロック内のシャッフル処理を行うものである。

【０３５３】そして、この第７の具体例によるデータ記録／再生装置は、上述したような第６の具体例によるデータ記録／再生装置において、前記所定の処理として、を行うことを特徴としている。

【０３５４】図２９は、第２の実施形態における第７の具体例によるデータ記録／再生装置の機能を説明するために示している図である。

【０３５５】すなわち、この第７の具体例による手法では、可搬型記憶媒体１００上のユーザー領域のファイルｆｉｌｅ．ｔｅｘｔのデータが記録されている領域で、クラスタ単位でシャッフル処理を行うと共に、その処理情報をシャッフル処理の情報（パラメータ等）を可搬型記憶媒体１００上のシステム管理領域に記録するようにしている。

【０３５６】図３０は、第２の実施形態における第８の具体例によるデータ記録／再生装置の機能を説明するために示している図である。

【０３５７】すなわち、この第８の具体例による手法では、前述した第７の具体例による手法と同様にシャッフル処理を行うものであるが、その際可搬型記憶媒体１００上のユーザー領域のファイルｆｉｌｅ．ｔｅｘｔのデータが記録されている領域で、クラスタ内でブロック単位でシャッフル処理を行うと共に、その処理情報をシャッフル処理の情報（パラメータ等）を可搬型記憶媒体１００上のシステム管理領域に記録するようにしている。

【０３５８】そして、この第８の具体例によるデータ記録／再生装置は、上述したような第６の具体例によるデータ記録／再生装置において、前記所定の処理として、ブロック単位でシャッフル処理を行うことを特徴としている。

【０３５９】図３１は、第２の実施形態における第９の具体例によるデータ記録／再生装置の機能を説明するために示している図である。

【０３６０】すなわち、この第９の具体例による手法では、前述した第７の具体例による手法と同様にシャッフル処理を行うものであるが、その際可搬型記憶媒体１００上のユーザー領域のファイルｆｉｌｅ．ｔｅｘｔのデータが記録されている領域で、データ全体に対してシャッフル処理を行うと共に、その処理情報をシャッフル処理の情報（パラメータ等）を可搬型記憶媒体１００上のシステム管理領域に記録するようにしている。

【０３６１】そして、この第９の具体例によるデータ記録／再生装置は、上述したような第６の具体例によるデータ記録／再生装置において、前記所定の処理として、データ全体に対するシャッフル処理を行うことを特徴としている。

【０３６２】図３２は、第２の実施形態における第１０の具体例によるデータ記録／再生装置の機能を説明するために示している図である。

【０３６３】すなわち、この第１０の具体例による手法では、前述した第７の具体例による手法のようにシャッフル処理を行うのでなく、可搬型記憶媒体１００上のユーザー領域のファイルｆｉｌｅ．ｔｅｘｔのデータが記録されている領域で、データ全体に対して暗号化処理を行うと共に、その処理情報をアルゴリズムに関する情報（暗号鍵の情報等）として可搬型記憶媒体１００上のシステム管理領域に記録するようにしている。

【０３６４】そして、この第１０の具体例によるデータ記録／再生装置は、上述したような第６の具体例によるデータ記録／再生装置において、前記所定の処理として、データ全体に対する暗号化処理を行うことを特徴としている。

【０３６５】そして、第１１の具体例によるデータ記録／再生装置は、上述したような第７乃至第１０の具体例によるデータ記録／再生装置において、前記所定の処理として、前記ブロック内のシャッフル処理、ブロック単位でシャッフル処理、データ全体に対するシャッフル処理及びデータ全体に対する暗号化処理のうちの少なくとも２つ以上の処理を組み合わせたことを特徴としている。

【０３６６】（第１２の具体例）次に、図３３乃至図３８を用いて、本発明によるデータ記録／再生装置の第２の実施形態の第１２の具体例について説明する。

【０３６７】図３３は、第２の実施形態における第１２の具体例によるデータ記録／再生装置の構成を示すブロ

ック図である。

【０３６８】すなわち、このデータ記憶／再生装置１０１は、外部のＰＣ１１０と通信を行う通信部１０２と、この通信部１０２にそれぞれ内部バスを介して接続されている作業用メモリ部１０３、鍵データ記憶用メモリ部１０４、制御部１０５、復号化部１０６、暗号化部１０７、可搬型記憶媒体駆動部１０８、媒体判定部１０９（図示せず、第１の実施形態参照）、ハッシュ演算部６０１から構成される。

【０３６９】通信部１０２は、ＳＣＳＩ（Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ ＳｙｓｔｅｍＩｎｔｅｒｆａｃｅ）やイーサネット、シリアルケーブル等の通信ケーブル、あるいは赤外線などの無線を用いて、データ記録／再生装置外部のＰＣ１１０やワークステーションなどのデータ作成・編集装置とデータやコマンドのやり取りをする機能を持つ。

【０３７０】作業用メモリ１０３は、通信部１０２などから送られてきたデータや、各種処理の途中段階のデータをバッファリングすると共に、プログラムをロードするためのメモリである。

【０３７１】また、鍵データ格納用メモリ部１０４は、秘密情報、例えば、ＤＥＳ等の暗号鍵を格納するためのメモリである。

【０３７２】制御部１０５は、データ記憶／再生装置１０１の処理全体を制御する部分である。

【０３７３】復号化部１０６は、鍵データ格納用メモリ部１０４からデータを復号化するための情報を読み出し、データを復号化する。

【０３７４】同様に暗号化部１０７は、鍵データ格納用メモリ部１０４からデータを暗号化するための情報を読み出し、データを暗号化する。

【０３７５】また、可搬型記憶媒体駆動部１０８は、制御部１０５からの処理要求に応じ、当該データ記憶／再生装置１０１に装填される可搬型記憶媒体１００上の領域のデータの読み出し／書き込み（消去を含む）を行う。

【０３７６】なお、図示しない媒体判定部１０９では、当該データ記憶／再生装置１０１に装填される記憶媒体が、本発明による手法で記録されている可搬型記憶媒体１００であるか、それ以外の記憶媒体であるかを判定する。

【０３７７】ハッシュ演算部６０１は、データからハッシュ関数を用いてハッシュ値を演算する。

【０３７８】すなわち、この第１２の具体例によるデータ記録／再生装置は、上述したような第１の実施形態によるデータ記録／再生装置において、データを前記可搬型記録媒体１００に記録する処理において、データに所定のコード抽出処理を施して得られたコードをシステム管理領域に記録すると共に、前記可搬型記録媒体１００からデータを読み出すときに、前記所定のコード抽出処理を施して得られたコードを前記システム管理領域に記録されている前記コードと照合することを特徴としている。

【０３７９】そして、この第１２の具体例によるデータ記録／再生装置は、前述した第１乃至第１１の具体例によるデータ記録／再生装置とは独立しているが、それらと適宜に併用することも可能である。

【０３８０】通常、通信等で改竄検知に用いられている電子書名の方式は以下のようになっている。

【０３８１】電子署名の作成：データからハッシュ関数を用いてハッシュ値（電子署名では一般にメッセージダイジェストと呼ばれる）を取り出し、それを秘密鍵で暗号化し電子署名として保存。

検証：検証するデータからハッシュ関数を用いてハッシュ値を取り出す（Ｈ１）と共に、電子署名を公開鍵で復号化し、ダイジェストデータを取り出し（Ｈ２）、Ｈ１とＨ２を照合する。

【０３８２】しかるに、この第１２の具体例によるデータ記録／再生装置の場合は、このような電子書名の方式によるよりも簡単な手法でデータの改竄を検知することができる。

【０３８３】すなわち、この第１２の具体例による手法では、データからハッシュ関数を用いてハッシュ値を求め、それをシステム管理領域にデータファイルと対応づけて記録するようにしている。

【０３８４】なぜなら、データ管理領域は暗号化するため、ユーザーはシステム管理領域のハッシュ値を変更することはできないからである。

【０３８５】よって、この第１２の具体例による手法では、ユーザーがデータを書き換えても、システム管理領域に記録されているデータのハッシュ値と矛盾するので改竄を検知することができる。

【０３８６】図３４は、上記改竄検知法を用いたこの第１２の具体例による手法によるファイルシステムのＦＡＴ１６の場合のエントリ構成を示している図である。

【０３８７】この例では、１つのデータのＦＡＴリンク以下のようになる。

【０３８８】まず、開始クラスタ（ＩＤ）としてＦＡＴエントリ（ＩＤ）が１４からアクセスが開始され、ＦＨ＝１５でＦＡＴエントリ（ＩＤ）が１５に移行し、１０Ｈ＝１６でＦＡＴエントリ（ＩＤ）が１６に移行し、１１Ｈ＝１７でＦＡＴエントリ（ＩＤ）が１７に移行し、１２Ｈ＝１８でＦＡＴエントリ（ＩＤ）が１８に移行する。

【０３８９】なお、ＦＡＴエントリ（ＩＤ）が１８のＦＦＦＨは、ファイルの最後のクラスタである。

【０３９０】そして、ＦＡＴエントリ（ＩＤ）が１９と２０のところにハッシュ値が記録されている。

【０３９１】図３５は、上記改竄検知法を用いたこの第１２の具体例による手法を前述した第６の具体例による

手法に適用したファイルシステムの場合のエントリ構成を示している図である。

【０３９２】このＦＡＴエントリ（ＩＤ）構成は、図３５に示すように、開始クラスタＩＤ、最後のクラスタＩＤ、ハッシュ値、欠陥クラスタの個数、欠陥クラスタ１のＩＤ、欠陥クラスタ２のＩＤ等を有している。

【０３９３】図３６は、上記改竄検知法をを用いたこの第１２の具体例による手法を説明するディスク等の可搬型記録媒体上での概念図である。

【０３９４】すなわち、この第１２の具体例による手法では、可搬型記憶媒体１００上のユーザー領域のファイルｆｉｌｅ．ｔｅｘｔのデータが記録されている領域で、データからハッシュ関数を用いてハッシュ値を求め、そのハッシュ値をシステム管理領域にデータファイルと対応づけて記録するようにしている。

【０３９５】図３７は、この第１２の具体例によるデータ書き込み時のフローチャートである。

【０３９６】この処理フローは、図３７に示すように、まず、データが入力されると、データからハッシュ関数を用いてハッシュ値を求め、そのハッシュ値をＦＡＴ中に記録する（ステップＳ１０１，Ｓ１０２）。

【０３９７】次に、可搬型記憶媒体上にデータを記録する（ステップＳ１０３）。

【０３９８】次に、ＦＡＴ及びディレクトリエントリの情報を更新すると共に、システム管理用データを暗号化して可搬型記憶媒体上にデータを記録した後、終了する（ステップＳ１０４，Ｓ１０５，Ｓ１０６）。

【０３９９】図３８は、この第１２の具体例によるデータ続み出し時のフローチャートである。

【０４００】この処理フローは、図３８に示すように、まず、ファイル名が入力されると、システム管理用データを読み出して復号化する（ステップＳ３１，Ｓ３２）。

【０４０１】次に、ＦＡＴ及びディレクトリエントリの情報を取得すると共に、可搬型記憶媒体からデータを読み出す（ステップＳ３３，Ｓ３４）。

【０４０２】次に、データからハッシュ関数を用いてハッシュ値を求め、システム管理用データ中に記録されているハッシュ値と照合する（ステップＳ３５）。

【０４０３】次に、ハッシュ値が一致しているか否かを判定し、ハッシュ値が一致していればそのまますする終了するが、ハッシュ値が一致していなければデータが改竄されていることを通知した後、終了する（ステップＳ３６，Ｓ３７，Ｓ３８）。

【０４０４】

【発明の効果】従って、以上説明したように、本発明によれば、画像等の大容量のデータを可搬型記憶媒体に格納する場合に、データ内容の秘匿性、真正性を確保し、且つデータの不正な消去・破壊を含めた改竄を防止でき、且つ高速な処理を実現できるデータ記録／再生装置を提供することができる。

【図面の簡単な説明】

【図１】図１は、第１の実施形態におけるデータ記憶／再生装置の構成を示すブロック図である。

【図２】図２は、本発明の変形例におけるデータ記憶／再生装置の構成を示すブロック図である。

【図３】図３は、一般的なファイルシステムを説明するための図である。

【図４】図４は、本発明による第１の実施形態を用いられる可搬型記憶媒体１００上の構成を示す図である。

【図５】第１の実施形態における記憶媒体上の構成（システム管理領域の一部を暗号化）を説明するための図である。

【図６】図６は、本発明による第１の実施形態におけるデータ読み出し時の処理の流れを示すフローチャートである。

【図７】図７は、第１の実施形態で可搬型記憶媒体１００へ初めてアクセスしてデータを読み出すときの処理の流れを示すフローチャートである。

【図８】図８は、第１の実施形態でデータを書き込むときの処理の流れを示すフローチャートである。

【図９】図９は、第１の実施形態で可搬型記憶媒体１００へ初めてアクセスしてデータを書き込むときの処理の流れを示すフローチャートである。

【図１０】図１０の（ａ）は、第１の実施形態で可搬型記憶媒体１００へ初めてアクセスしてデータを書き込むときの処理の流れを示す他のフローチャートであり、図１０の（ｂ）は、第１の実施形態で可搬型記憶媒体１００の排出要求があったときの処理の流れを示すフローチャートである。

【図１１】図１１は、本発明による第２の実施形態における５つの手法に対応するＭＳ－ＤＯＳ　ＦＡＴ１６ファイルシステムのファイル管理手法を説明するための図である。

【図１２】図１２は、第２の実施形態における第１の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【図１３】図１３は、第２の実施形態における第１の具体例による手法に基づいたＦＡＴ１６ファイルシステムにおけるデータ管理形態を示す図である。

【図１４】図１４は、通常のファイルシステムを用いた場合に、システム管理領域とユーザー領域とを有する可搬型記録媒体のユーザー領域にデータが記録されるときの例を参考的に示す図である。

【図１５】図１５は、第２の実施形態における第１の具体例による手法に基づいたデータの記録形態を示す図である。

【図１６】図１６は、第２の実施形態における第１の具体例による場合の１つのデータのＦＡＴリンクをず１４の一部と対応付けて示す図である。

41

【図１７】図１７は、第２の実施形態における第１の具体例によるファイルシステムを用いた場合に、システム管理領域とユーザー領域とを有する可搬型記録媒体のユーザー領域にデータが記録されるときの例を示す図である。

【図１８】図１８は、第２の実施形態における第２の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【図１９】図１９の（ａ），（ｂ）は、通常の場合のＦＡＴリンクの初期化状態と、この第２の具体例による手法に基づいたＦＡＴリンクの初期化状態とを対比させて示す図である。

【図２０】図２０は、第２の実施形態における第３の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【図２１】図２１は、この第３の具体例による手法を説明するための概念図である。

【図２２】図２２は、この第３の具体例による手法を説明するためのフローチャートである。

【図２３】図２３は、第２の実施形態における第４の具体例によるデータ記録／再生装置の機能を説明するためのフローチャートである。

【図２４】図２４は、第２の実施形態における第５の具体例によるデータ記録／再生装置の機能を説明するためにＦＡＴエントリ構成を示している図である。

【図２５】図２５の（ａ），（ｂ）は、第２の実施形態における第１の具体例に準じた場合のＦＡＴファイルシステムと、第２の実施形態における第５の具体例による手法に基づいたファイルシステムとを対比させて示している図である。

【図２６】図２６は、第２の実施形態における第６乃至第１１の具体例によるデータ記録／再生装置の機能を共通に説明するためにＦＡＴエントリ構成を示している図である。

【図２７】図２７は、第２の実施形態における第６乃至第１１の具体例によるデータ記録／再生装置の機能を共通に説明するためのフローチャートである。

【図２８】図２８は、第２の実施形態における第７の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【図２９】図２９は、第２の実施形態における第７の具体例によるデータ記録／再生装置の機能を説明するために示している図である。

【図３０】図３０は、第２の実施形態における第８の具体例によるデータ記録／再生装置の機能を説明するために示している図である。

【図３１】図３１は、第２の実施形態における第９の具体例によるデータ記録／再生装置の機能を説明するために示している図である。

42

【図３２】図３２は、第２の実施形態における第１０の具体例によるデータ記録／再生装置の機能を説明するために示している図である。

【図３３】図３３は、第２の実施形態における第１２の具体例によるデータ記録／再生装置の構成を示すブロック図である。

【図３４】図３４は、第２の実施形態における第１２の具体例による手法によるファイルシステムのＦＡＴ１６の場合のエントリ構成を示している図である。

【図３５】図３５は、第２の実施形態における第１２の具体例による手法を前述した第６の具体例による手法に適用したファイルシステムの場合のエントリ構成を示している図である。

【図３６】図３６は、第２の実施形態における第１２の具体例による手法を説明するディスク等の可搬型記録媒体上での概念図である。

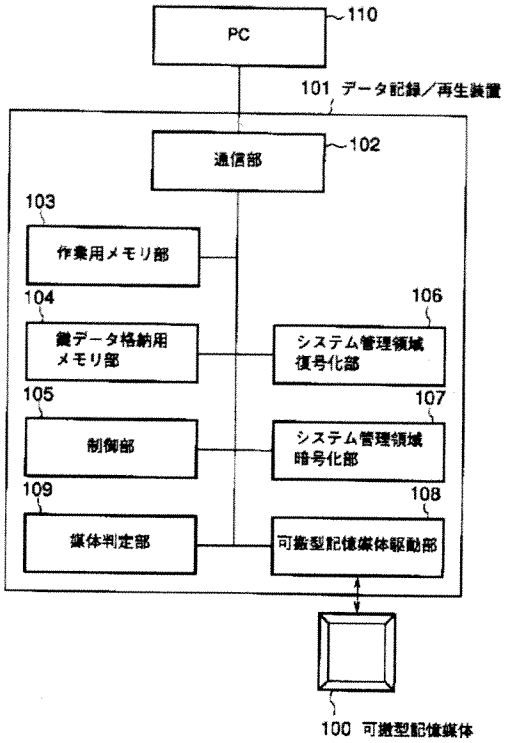
【図３７】図３７は、第２の実施形態における第１２の具体例によるデータ書き込み時のフローチャートである。

【図３８】図３８は、第２の実施形態における第１２の具体例によるデータ続み出し時のフローチャートである。

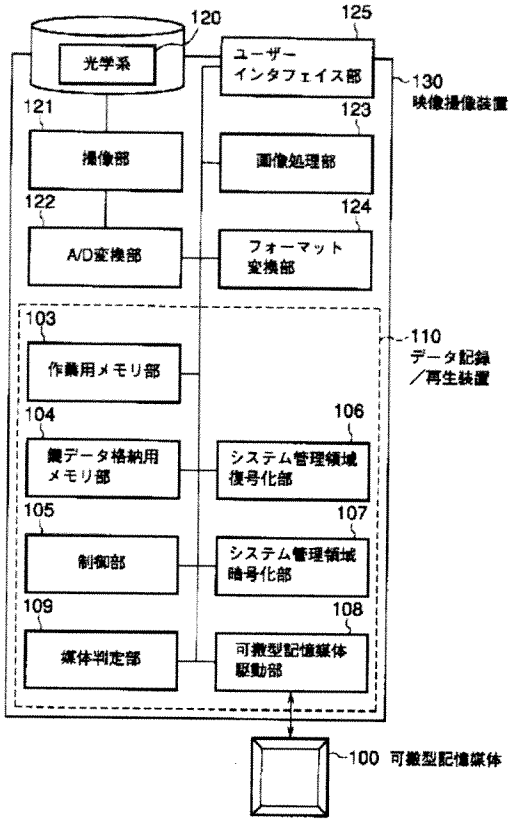
【符号の説明】

１００…可搬型記憶媒体、
１０１…データ記憶／再生装置、
１１０…ＰＣ、
１０２…通信部、
１０３…作業用メモリ部、
１０４…鍵データ記憶用メモリ部、
１０５…制御部、
１０６…復号化部、
１０７…暗号化部、
１０８…可搬型記憶媒体駆動部、
１０９…媒体判定部、
１３０…映像撮像装置、
１２０…光学系、
１２０…撮像部、
１２２…Ａ／Ｄ変換部、
１２３…画像処理部、
１２４…フォーマット変換部、
１２５…ユーザーインタフエイス部。
２０１…データ分割部、
２０２…クラスタ選択部
３０１…クラスタ選択部、
３０２…乱数発生部、
４０１…クラスタ照合部、
４０２…乱数発生部、
５０１…シャッフル処理部、
６０１…ハッシュ演算部。

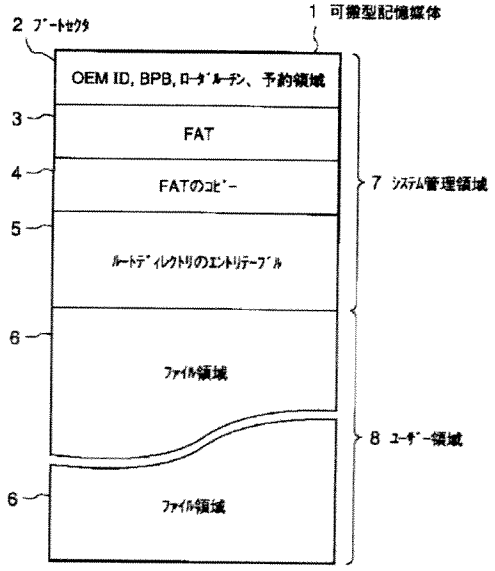
【図１】


PC
110
101 データ記録／再生装置
通信部
102
103
作業用メモリ部
104
鍵データ格納用メモリ部
106
システム管理領域復号化部
105
制御部
107
システム管理領域暗号化部
109
媒体判定部
108
可搬型記憶媒体駆動部
100 可搬型記憶媒体

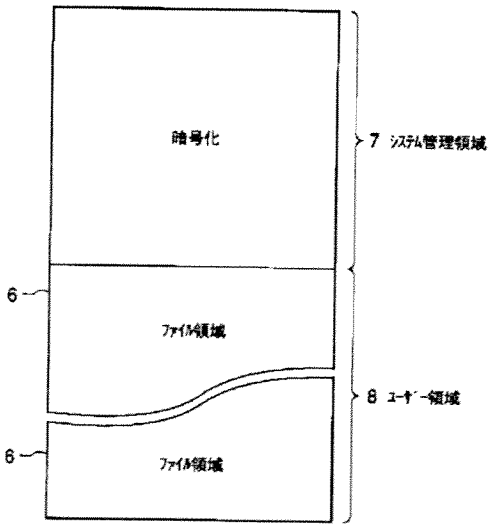
【図２】


120
125
光学系
ユーザーインタフェイス部
130
映像撮像装置
121
123
撮像部
画像処理部
122
124
A/D変換部
フォーマット変換部
103
作業用メモリ部
110
データ記録／再生装置
104
106
鍵データ格納用メモリ部
システム管理領域復号化部
105
107
制御部
システム管理領域暗号化部
109
108
媒体判定部
可搬型記憶媒体駆動部
100 可搬型記憶媒体

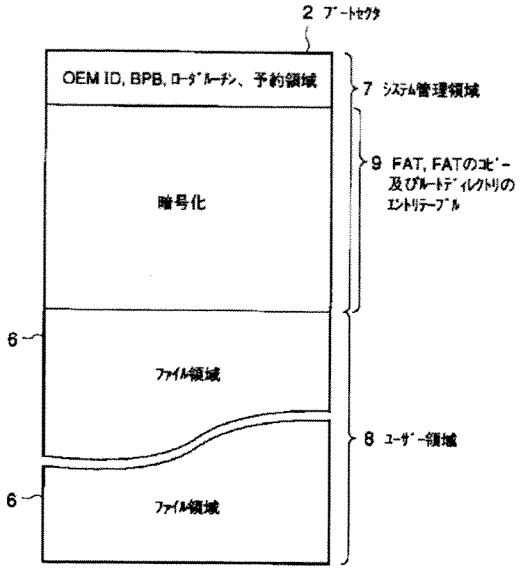
【図３】


1 可搬型記憶媒体
2 ﾌﾞｰﾄｾｸﾀ
OEM ID, BPB, ﾙｰﾄﾃﾞｨﾚｸﾄﾘｴﾝﾄﾘ、予約領域
3
FAT
4
FATのｺﾋﾟｰ
5
ﾙｰﾄﾃﾞｨﾚｸﾄﾘのｴﾝﾄﾘﾃｰﾌﾞﾙ
6
ﾌｧｲﾙ領域
7 ｼｽﾃﾑ管理領域
8 ﾕｰｻﾞｰ領域
6
ﾌｧｲﾙ領域

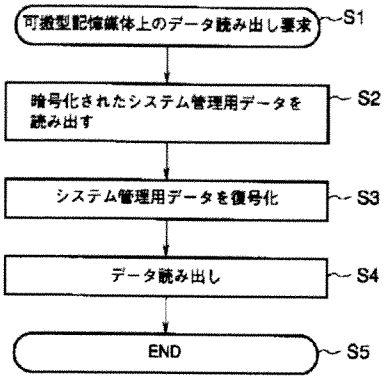
【図４】


暗号化
7 ｼｽﾃﾑ管理領域
6
ﾌｧｲﾙ領域
8 ﾕｰｻﾞｰ領域
6
ﾌｧｲﾙ領域

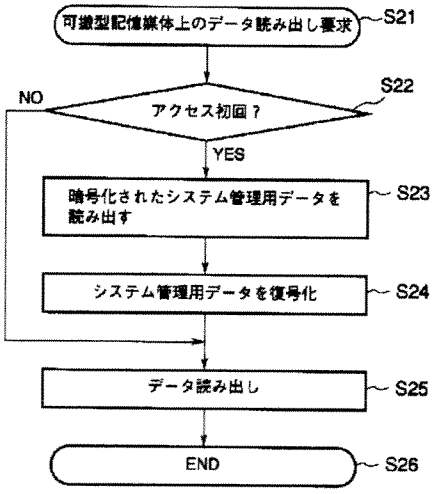
【図5】



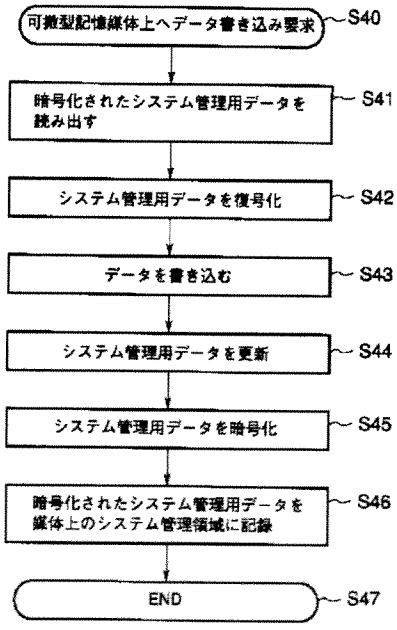
【図6】



【図7】



【図8】

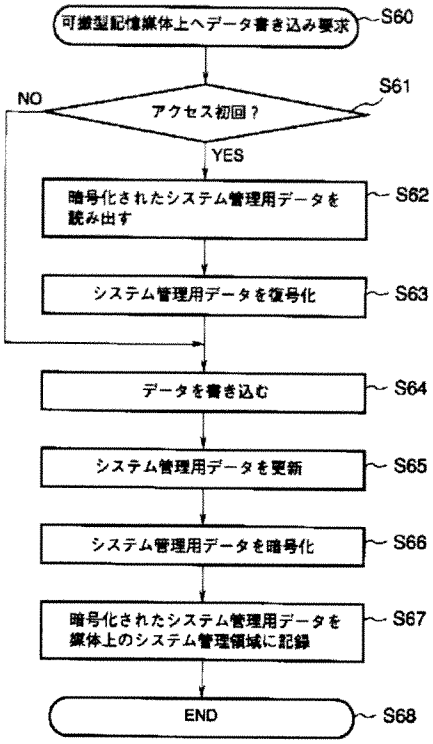


【図24】

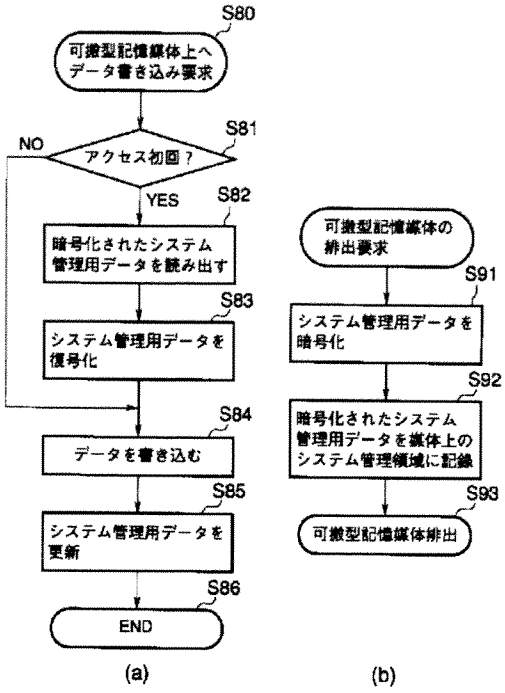
FATエントリ(ID)

.....	開始のクラスタID	最後のクラスタID	欠陥クラスタの個数	欠陥クラスタ1のID	欠陥クラスタ2のID	.....

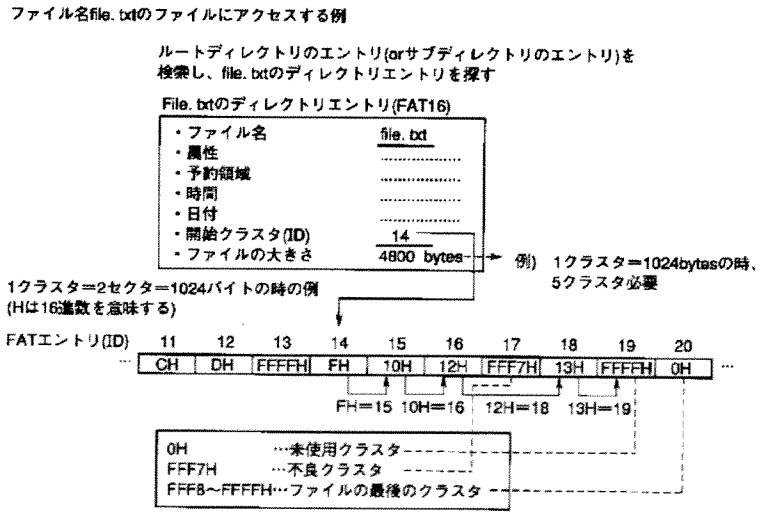
【図９】



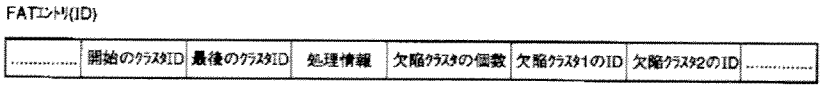
【図１０】



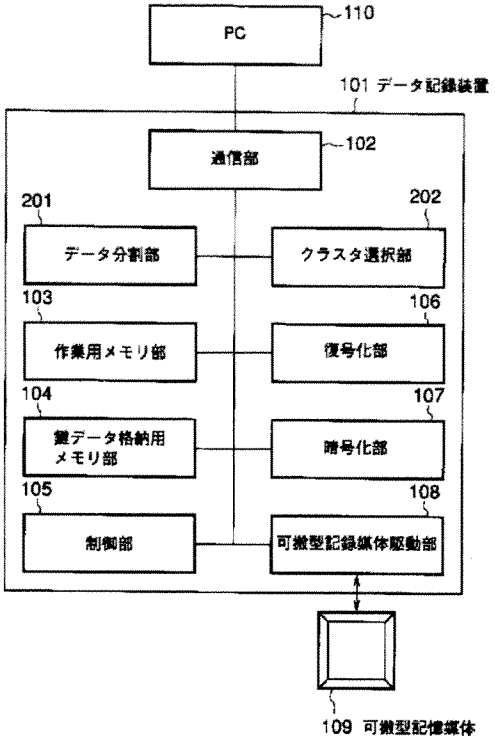
【図１１】



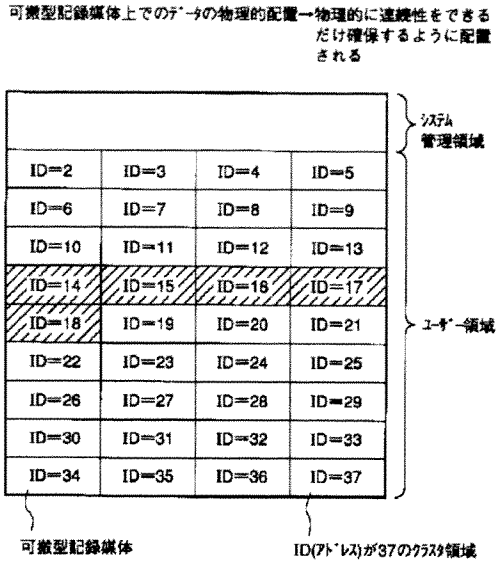
【図２６】



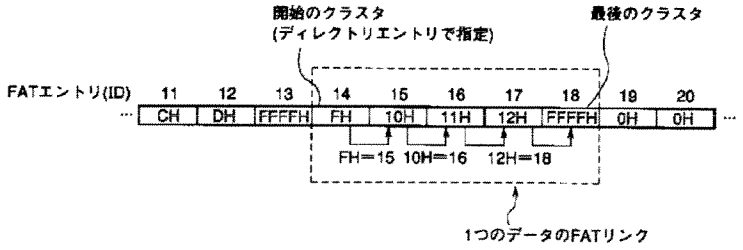
【図１２】



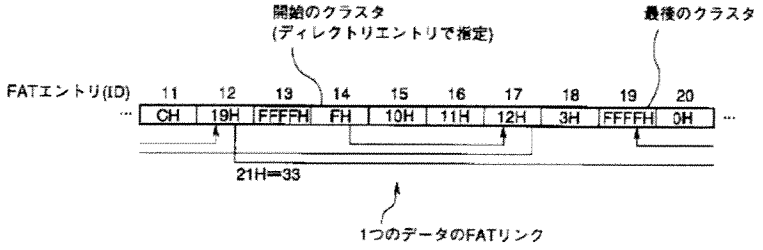
【図１４】



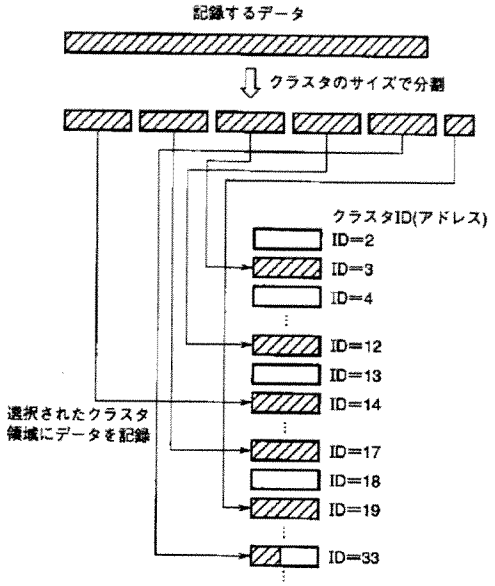
【図１３】



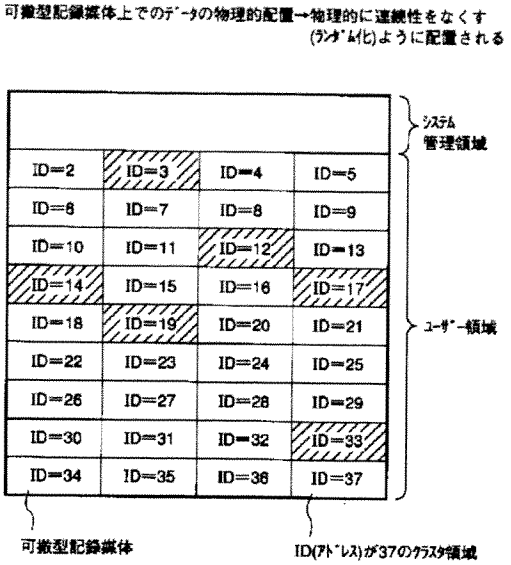
【図１６】



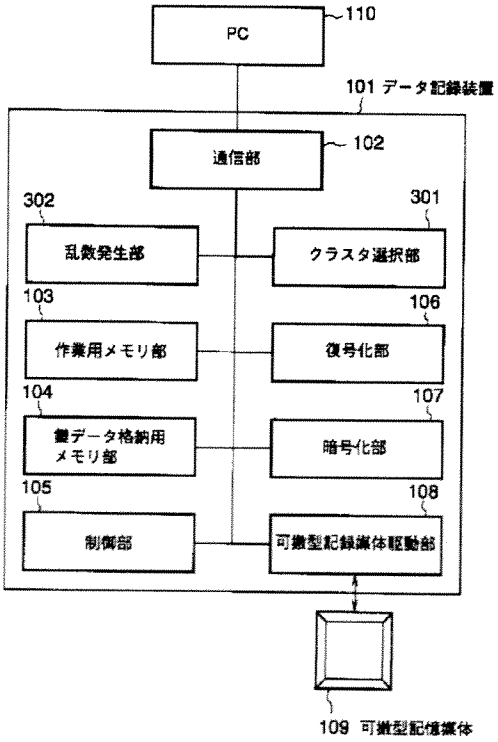
【図15】



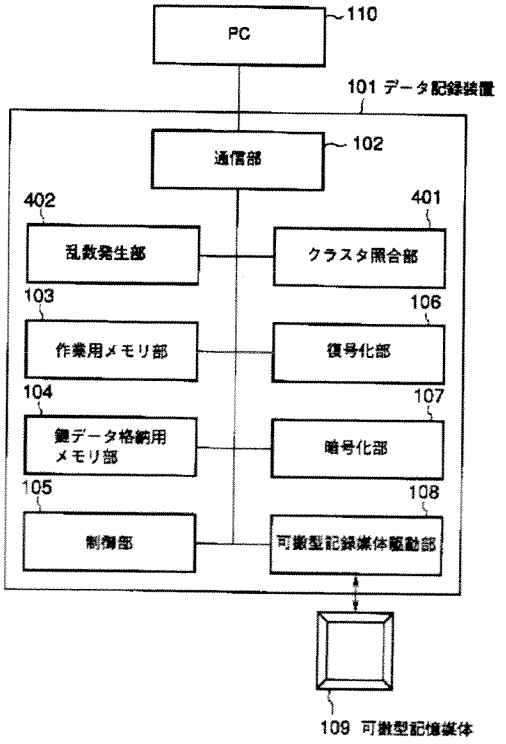
【図17】



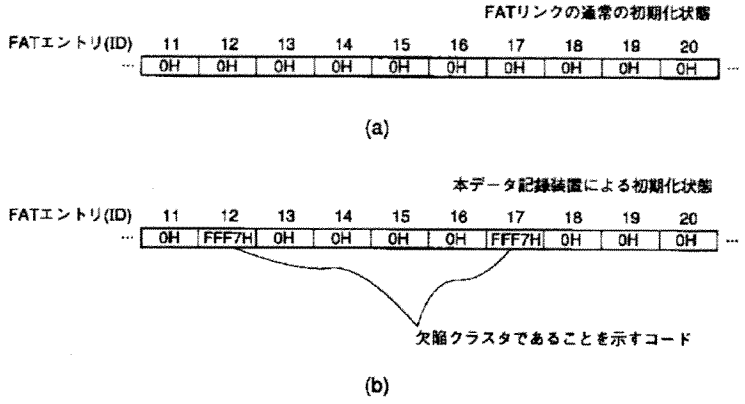
【図18】



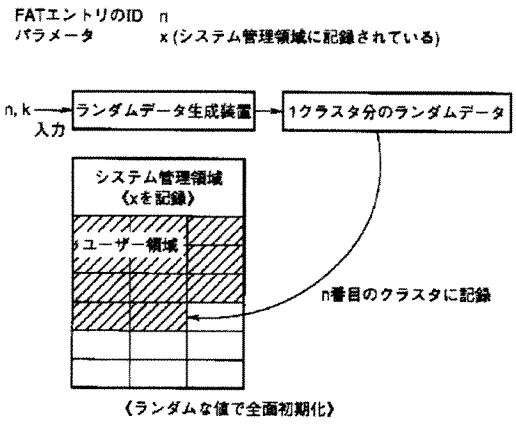
【図20】



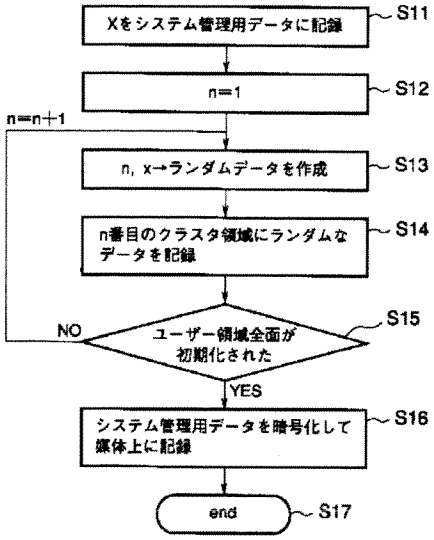
【図１９】



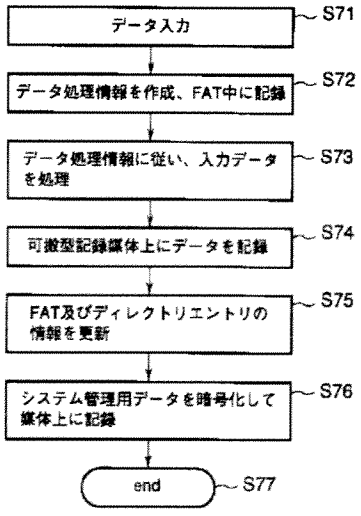
【図２１】



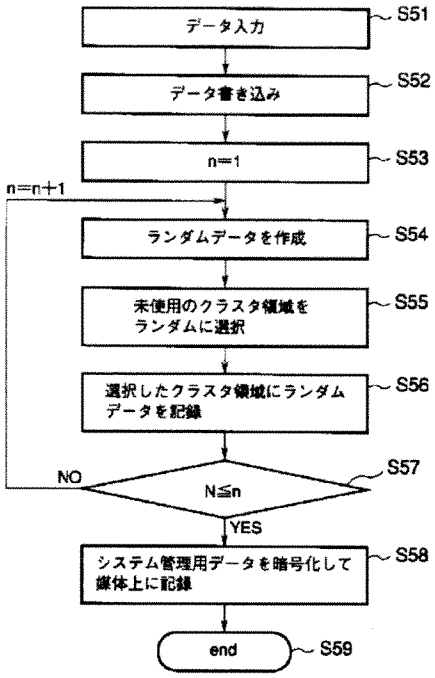
【図２２】



【図２７】

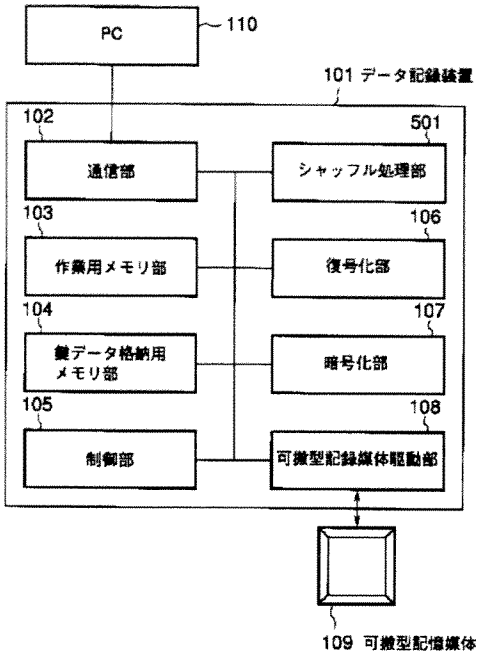


【図２３】

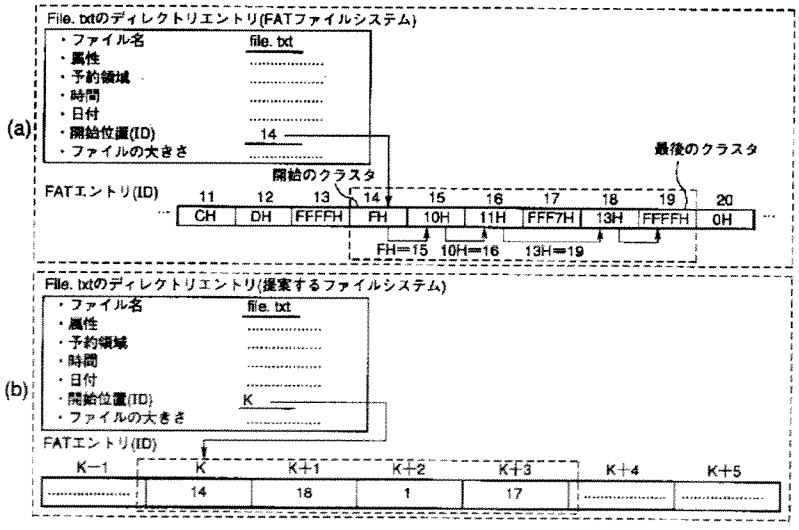


※Nは、ランダムデータを書き込むクラスタ領域数

【図２８】



【図２５】

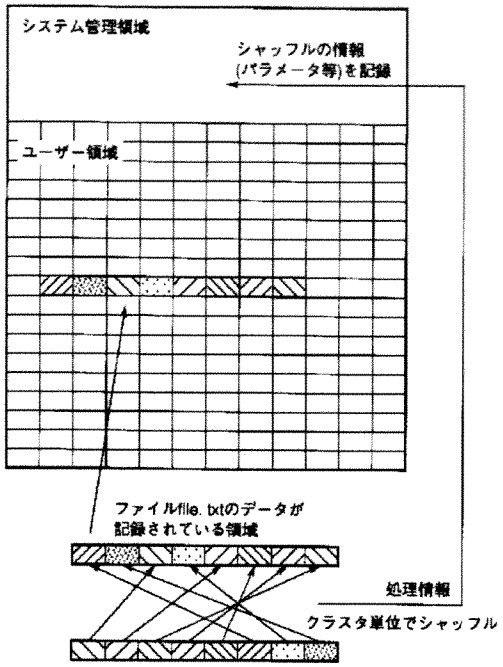


【図３５】

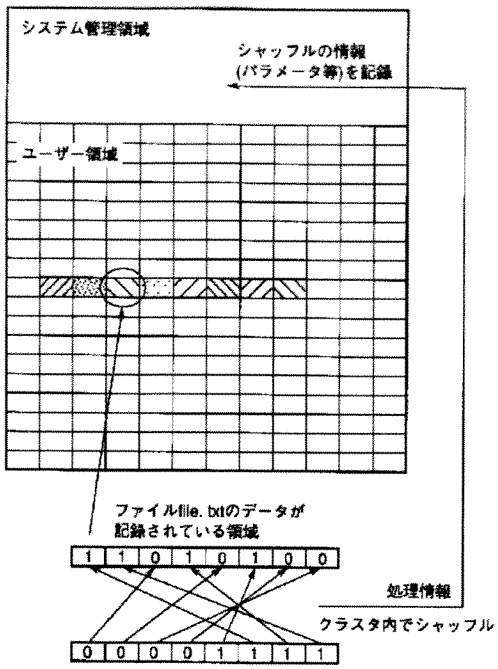
FATエントリ(ID)

.....	開始のクラスタID	最後のクラスタID	ハッシュ値	欠陥クラスタの個数	欠陥クラスタ1のID	欠陥クラスタ2のID	.....

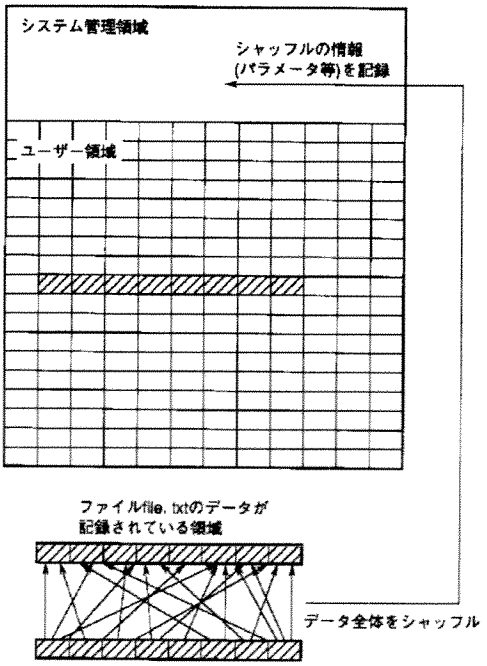
【図２９】



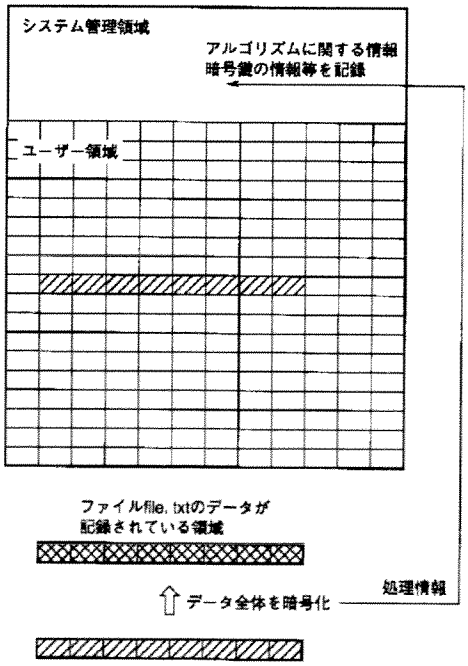
【図３０】



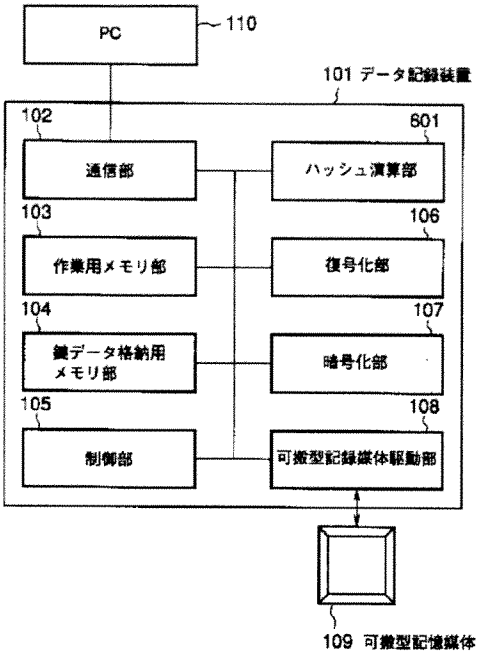
【図３１】



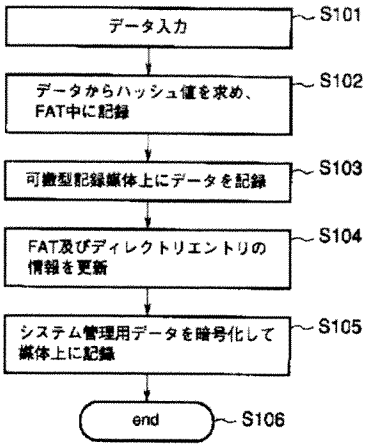
【図３２】



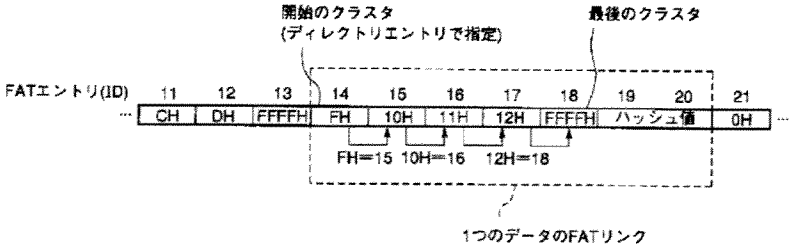
【図３３】


PC
110
101 データ記録装置
102
601
通信部
ハッシュ演算部
103
106
作業用メモリ部
復号化部
104
107
鍵データ格納用
メモリ部
暗号化部
105
108
制御部
可搬型記録媒体駆動部
109 可搬型記憶媒体

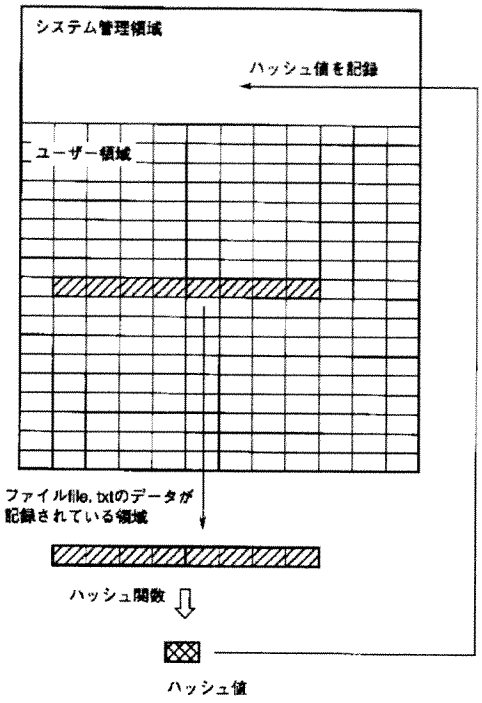
【図３７】


データ入力
S101
データからハッシュ値を求め、
FAT中に記録
S102
可搬型記録媒体上にデータを記録
S103
FAT及びディレクトリエントリの
情報を更新
S104
システム管理用データを暗号化して
媒体上に記録
S105
end
S106

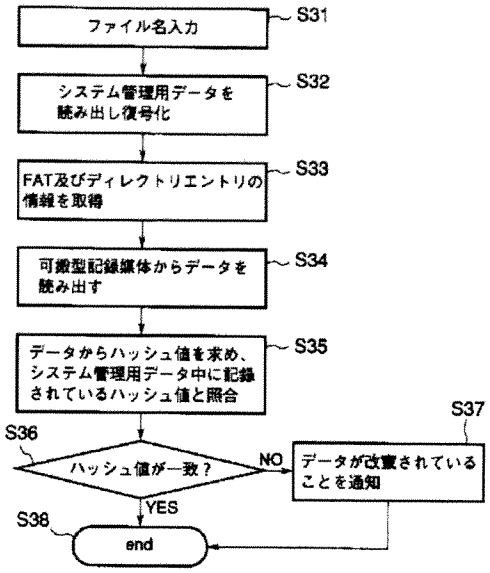
【図３４】


開始のクラスタ
(ディレクトリエントリで指定)
最後のクラスタ
FATエントリ(ID)
11 12 13 14 15 16 17 18 19 20 21
CH DH FFFFH FH 10H 11H 12H FFFFH ハッシュ値 0H
FH=15 10H=16 12H=18
1つのデータのFATリンク

【図３６】



【図３８】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｎ　5/92		Ｈ０４Ｎ　5/92	Ｈ